aws

Guía para desarrolladores

Amazon DocumentDB



Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon DocumentDB: Guía para desarrolladores

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Las marcas comerciales y la imagen comercial de Amazon no se pueden utilizar en relación con ningún producto o servicio que no sea de Amazon, de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas registradas que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, conectados o patrocinados por Amazon.

Table of Contents

Qué es Amazon DocumentDB 1
Descripción general de 1
Clústeres 3
instancias 4
Regiones y AZs 8
Regions 8
Zonas de disponibilidad 8
Precios 11
Prueba gratuita 11
Supervisión 11
Interfaces 12
Consola de administración de AWS 12
AWS CLI 12
Controladores de MongoDB 12
Siguientes pasos 13
Cómo funcionan 13
Puntos de conexión de Amazon DocumentDB 15
Compatibilidad con TLS 19
Almacenamiento de Amazon DocumentDB 20
Replicación de Amazon DocumentDB 21
Fiabilidad de Amazon DocumentDB 21
Opciones de preferencia de lectura 22
Eliminaciones de TTL 27
Recursos facturables 28
¿Qué es una base de datos de documentos? 31
Casos de uso 31
Descripción de documentos 32
Trabajo con documentos 38
Guía de introducción 51
Requisitos previos 51
Paso 1: creación de un clúster 53
Paso 2: Conexión al clúster 56
Paso 3: insertar y consultar datos 57
Paso 4: explorar 59

Inicio rápido a usar CloudFormation 60
Requisitos previos 60
Permisos de IAM necesarios 61
Par de EC2 claves de Amazon 61
Lanzamiento de una pila de CloudFormation de Amazon DocumentDB 61
Acceso al clúster de Amazon DocumentDB 67
Protección de terminación y protección de eliminación 67
Compatibilidad con MongoDB 68
Compatibilidad con MongoDB 8.0 68
Novedades de Amazon DocumentDB 8.0 68
Introducción a Amazon DocumentDB 69
Actualización o migración a Amazon DocumentDB 5.0 u 8.0 70
Diferencias funcionales 70
Compatibilidad con MongoDB 5.0 70
Novedades de Amazon DocumentDB 5.0 71
Introducción a Amazon DocumentDB 5.0 69
Actualización o migración a Amazon DocumentDB 5.0 70
Diferencias funcionales 70
Compatibilidad con MongoDB 4.0 74
Características de Amazon DocumentDB 4.0 74
Introducción a Amazon DocumentDB 4.0 75
Actualización o migración a Amazon DocumentDB 4.0 76
Diferencias funcionales 76
Transacciones 78
Requisitos 78
Prácticas recomendadas 79
Limitaciones 79
Supervisión y diagnóstico 80
Nivel de aislamiento de transacciones 81
Casos de uso 81
Transacciones con varios estados de cuenta 81
Transacciones de varias recopilaciones 83
Ejemplos de API de transacciones para la API de devolución de llamada 85
Ejemplos de API de transacciones para la API de Core 85
Comandos admitidos 119
Capacidades no compatibles 120

Sesiones ... 120
Coherencia causal ... 121
Reintento de las escrituras ... 122
Errores de la transacción ... 122
Prácticas recomendadas ... 124
Directrices operativas básicas ... 124
Determinación del tamaño de las instancias ... 126
Uso de índices ... 127
Creación de índices ... 127
Selectividad de índice ... 128
Impacto de los índices en los datos de escritura ... 128
Identificación de índices que faltan ... 129
Identificación de índices no utilizados ... 129
Prácticas recomendadas de seguridad ... 129
Optimización de costos ... 130
Uso de métricas para identificar los problemas de rendimiento ... 130
Visualización de métricas de rendimiento ... 131
Configurar una CloudWatch alarma ... 131
Evaluación de las métricas de rendimiento ... 131
Evaluación del uso de instancias de Amazon DocumentDB con métricas CloudWatch ... 133
Ajuste de consultas ... 135
TTL y cargas de trabajo de series temporales ... 135
Migraciones ... 136
Uso de grupos de parámetros de clúster ... 136
Consultas de canalización de agregación ... 136
`batchInsert` y `batchUpdate` ... 137
Diferencias funcionales con MongoDB ... 138
Beneficios funcionales de Amazon DocumentDB ... 138
Transacciones implícitas ... 138
Diferencias funcionales actualizadas ... 139
Indexación de matrices ... 140
Índices de varias claves ... 141
Caracteres nulos en cadenas ... 142
Control de acceso con base en roles ... 142
Indexación de `$regex` ... 142
Proyección para documentos anidados ... 143

Diferencias funcionales con MongoDB 143
$vectorSearchoperador 144
OpCountersCommand 144
Bases de datos de administración y colecciones 144
cursormaxTimeMS 144
explain() 144
Compilaciones de índices 145
Búsqueda con una clave vacía en la ruta 145
API, operaciones y tipos de datos de MongoDB 145
Utilidades de mongodump y mongorestore 146
Ordenación de los resultados 146
Reintento de las escrituras 146
Índices dispersos 147
Uso de $elemMatch dentro de una expresión $all 147
Dólar($) y punto(.) en los nombres de campos 148
$lookup 148
$natural y clasificación inversa 152
APIsMongoDB, operaciones y tipos de datos compatibles 153
Comandos de la base de datos 154
Comandos administrativos 154
Agregación 156
Autenticación 156
Comandos de diagnóstico 157
Operaciones de consulta y escritura 158
Comandos para la administración de roles 159
Comandos de sesiones 159
Administración de usuarios 160
Comandos de partición 161
Operadores de consulta y proyección 163
Operadores de matrices 163
Operadores Bitwise 164
Operador de comentarios 164
Operadores de comparación 164
Operadores de elementos 165
Operadores de consulta de evaluación 165
Logical operators (Operadores lógicos) 166

Operadores de proyección ... 166
Operadores de actualización ... 166
Operadores de matrices ... 167
Operadores Bitwise ... 167
Operadores de campo ... 167
Modificadores de actualización ... 168
Geospatial (Geoespacial) ... 169
Especificadores de geometría ... 169
Selectores de consultas ... 169
Métodos de cursor ... 170
Operadores de canalización de agregación ... 172
Expresiones de acumulación ... 173
Operadores aritméticos ... 175
Operadores de matrices ... 176
Operadores booleanos ... 177
Operadores de comparación ... 177
Operadores de expresiones condicionales ... 177
Operador de tipos de datos ... 178
Operador de tamaño de datos ... 178
Operadores de fechas ... 178
Operador literal ... 180
Operador de combinación ... 180
Operador natural ... 180
Operadores de establecimiento ... 181
Operadores de etapa ... 181
Operadores de cadena ... 184
Variables del sistema ... 185
Operador de búsqueda de texto ... 185
Operadores de conversión de tipos ... 186
Operadores de variables ... 186
Operadores misceláneos ... 187
Tipos de datos ... 187
Índices y propiedades de índices ... 188
Índices ... 189
Propiedades de índices ... 189
IA generativa ... 191

SageMaker Lienzo ... 191
¿Cómo crear modelos de aprendizaje automático sin código con AI Canvas? SageMaker .. 191
Configuración del dominio y el perfil de usuario de AI SageMaker ... 192
Configuración de los permisos de acceso de IAM para Amazon DocumentDB SageMaker y AI Canvas ... 192
Creación de usuarios y roles de bases de datos para SageMaker AI Canvas ... 193
Regiones disponibles ... 193
Búsqueda vectorial ... 194
Inserción de vectores ... 195
Creación de un índice vectorial ... 195
Obtención de una definición de índice ... 200
Consulta de vectores ... 201
Características y limitaciones ... 206
Prácticas recomendadas ... 207
Migración a DocumentDB ... 208
Guía de inicio rápido ... 208
Preparación del origen de DMS ... 208
Configuración de DMS ... 209
Habilitación de la compresión de DocumentDB ... 209
Creación de una tarea de replicación ... 209
Monitorear el progreso ... 210
Información adicional ... 210
Runbook de migración ... 210
Compatibilidad ... 211
Detección de la carga de trabajo ... 215
Migración de índices ... 218
Migración de usuario ... 220
Migración de datos ... 221
Supervisión ... 234
Validación ... 237
Migración desde Couchbase Server ... 242
Introducción ... 242
Comparación con Amazon DocumentDB ... 242
Discovery ... 245
Planificación ... 251
Migración ... 254

Validación ... 262
Actualización de DocumentDB ... 267
Fechas de soporte de la versión del motor ... 267
Actualización de la versión del motor de Amazon DocumentDB ... 268
Requisitos previos y limitaciones de la MVU ... 269
Prácticas recomendadas para actualizaciones de la versión principal locales ... 270
Actualización local de la versión principal ... 276
Diferencias entre los clústeres actualizados de Amazon DocumentDB 3.6 o 4.0 a 5.0 y los nuevos clústeres de Amazon DocumentDB 5.0 ... 279
Solución de problemas de una actualización local de la versión principal ... 279
Actualización mediante AWS DMS ... 280
Paso 1: habilitación de los flujos de cambios ... 281
Paso 2: modificación de la duración de la retención de los flujos de cambios ... 281
Paso 3: migración de los índices ... 281
Paso 4: Crear una AWS DMS instancia de replicación ... 283
Paso 5: Crear un punto final AWS DMS de origen ... 285
Paso 6: Crear un punto final AWS DMS de destino ... 287
Paso 7: crear y ejecutar una tarea de migración ... 289
Paso 8: cambiar el punto de conexión de origen de la aplicación al clúster de Amazon DocumentDB de destino ... 291
Soporte extendido ... 292
Información general del soporte extendido ... 293
Precios del Soporte extendido ... 294
Responsabilidades ... 294
Seguridad ... 295
Administración de contraseñas con AWS Secrets Manager ... 296
Limitaciones de la integración de Secrets Manager con Amazon DocumentDB ... 297
Descripción general de la administración de las contraseñas de los usuarios principales con AWS Secrets Manager ... 297
Hacer cumplir la administración de Amazon DocumentDB de la contraseña del usuario principal en AWS Secrets Manager ... 298
Administración de la contraseña del usuario principal para un clúster con Secrets Manager ... 298
Protección de los datos ... 299
Cifrado a nivel de campo del lado del cliente ... 300
Cifrado de datos en reposo ... 308

Cifrado de datos en tránsito ... 314
Administración de claves ... 325
Gestión de identidad y acceso ... 325
Público ... 326
Autenticación con identidades ... 326
Administración del acceso con políticas ... 327
Cómo funciona Amazon DocumentDB con IAM ... 329
Ejemplos de políticas basadas en identidades ... 336
Resolución de problemas ... 339
Administración de permisos de acceso para los recursos de Amazon DocumentDB ... 341
Uso de políticas basadas en identidades (políticas de IAM) ... 347
AWS políticas administradas para Amazon DocumentDB ... 352
Referencia sobre los permisos de la API de Amazon DocumentDB ... 371
Autenticación mediante la identidad de IAM ... 380
Introducción a los roles y usuarios de IAM ... 381
Configuración de tipos de cómputo ... 384
Supervisión de solicitudes de autenticación ... 385
Uso de la autenticación de IAM ... 385
Controladores compatibles con IAM ... 385
Preguntas frecuentes sobre la autenticación de identidad de IAM ... 386
Administración de usuarios de Amazon DocumentDB ... 387
Usuario principal y usuario `serviceadmin` ... 387
Creación de usuarios adicionales ... 388
Rotación automática de contraseñas ... 390
Control de acceso basado en roles ... 391
Conceptos de RBAC ... 392
Introducción a los roles integrados de RBAC ... 394
Introducción a los roles definidos por el usuario de RBAC ... 397
Conexión a Amazon DocumentDB como un usuario ... 402
Comandos comunes ... 404
Diferencias funcionales ... 409
Límites de las s ... 409
Acceso a la base de datos mediante el control de acceso basado en roles ... 409
Registro y supervisión ... 418
Actualización de certificados ... 419
Actualización de la aplicación y del clúster de Amazon DocumentDB ... 419

Rotación automática de certificados del servidor 424
Solución de problemas 425
Preguntas frecuentes 425
Actualización de los certificados: GovCloud 432
Actualización de la aplicación y del clúster de Amazon DocumentDB 419
Solución de problemas 425
Preguntas frecuentes 425
Validación de conformidad 445
Resiliencia 446
Seguridad de la infraestructura 448
Puntos de conexión de VPC (AWS PrivateLink) 449
Consideraciones para los puntos de enlace de VPC 450
Disponibilidad por región 450
Creación de un punto de conexión de VPC de interfaz para la API de Amazon DocumentDB 451
Creación de una política de punto de conexión de VPC para la API de Amazon DocumentDB 452
Prácticas recomendadas de seguridad 453
Auditoría de eventos 454
Eventos admitidos 455
Habilitar auditorías 460
Deshabilitar auditorías 468
Acceso a los eventos 471
Filtrado de eventos de DML 471
Amazon VPC y Amazon DocumentDB 477
Clústeres de DocumentDB en una VPC 477
Acceso a un clúster en una VPC 491
Crear una VPC IPv4 exclusiva para un clúster 494
Creación de una VPC de pila doble para un clúster 501
Copia de seguridad y restauración 512
Conceptos de copia de seguridad y restauración 513
Descripción del uso de almacenamiento de copias de seguridad en 516
Volcado, restauración, importación y exportación de datos 518
`mongodump` 518
`mongorestore` 519
`mongoexport` 520

mongoimport ... 520
Tutorial ... 521
Consideraciones sobre las instantáneas de clústeres ... 523
Almacenamiento de copia de seguridad ... 524
Intervalo de copia de seguridad ... 525
Backup retention period (Periodo de retención de copia de seguridad) ... 527
Copia del cifrado de instantáneas de clúster ... 527
Diferencias entre las instantáneas automáticas y manuales ... 528
Creación de una instantánea manual del clúster ... 530
Copia de una instantánea de clúster ... 533
Copia de instantáneas compartidas ... 534
Copiar instantáneas de un lado a otro Regiones de AWS ... 534
Limitaciones ... 534
Tratamiento del cifrado ... 535
Consideraciones relativas al grupo de parámetros ... 535
Copia de una instantánea de clúster ... 536
Compartir una instantánea de un clúster ... 545
Cómo compartir una instantánea cifrada ... 546
Uso compartido de una instantánea ... 550
Restauración de una instantánea del clúster ... 553
Restauración a un momento dado ... 560
Eliminación de una instantánea del clúster ... 567
Administración de Amazon DocumentDB ... 569
Información general sobre las tareas operativas ... 570
Agregación de una réplica a un clúster de Amazon DocumentDB ... 570
Descripción de clústeres e instancias ... 571
Creación de una instantánea de un clúster ... 573
Restauración a partir de una instantánea ... 574
Eliminación de una instancia de un clúster ... 576
Eliminación de un clúster ... 576
Clústeres globales ... 577
¿Qué es un clúster global? ... 577
¿Para qué sirven los clústeres globales? ... 577
¿Cuáles son las limitaciones actuales de los clústeres globales? ... 577
Guía de inicio rápido ... 578
Administración de clústeres globales ... 595

Conexión a clústeres globales ... 603
Supervisión de clústeres globales ... 603
Recuperación ante desastres ... 604
Administración de clústeres de ... 621
Descripción de clúster ... 622
Configuración del clúster ... 625
Configuración de almacenamiento en clústeres ... 627
Determinación del estado de un clúster ... 631
Ciclo de vida del clúster ... 632
Escalado de clústeres ... 676
Clonación de un volumen de clúster ... 679
Información general de tolerancia a errores para un clúster ... 692
Administración de instancias ... 694
Determinación del estado de una instancia ... 694
Ciclo de vida de la instancia ... 694
Administración de clases de instancias ... 719
Instancias respaldadas por NVMe ... 732
Administración de grupos de subredes ... 735
Creación de un grupo de subredes ... 736
Descripción de un grupo de subredes ... 742
Modificación de un grupo de subredes ... 745
Eliminación de un grupo de subredes ... 748
Alta disponibilidad y replicación ... 750
Escalado de lectura ... 750
Alta disponibilidad ... 750
Adición de réplicas de ... 752
Conmutación por error ... 752
Retraso de replicación ... 757
Administrar índices ... 759
Creación de índices de Amazon DocumentDB ... 759
Mantenimiento de índices de Amazon DocumentDB ... 765
Administración de la compresión de documentos ... 767
Administración de la compresión de documentos ... 768
Supervisión de la compresión de documentos ... 770
Administración de la compresión basada en diccionarios ... 771
Consideraciones sobre el rendimiento ... 772

Habilitar la compresión basada en diccionarios ... 772
Introducción ... 773
Supervisión ... 773
Administración de eventos ... 775
Visualización de categorías de eventos ... 775
Visualización de eventos de Amazon DocumentDB ... 778
Elección de regiones y zonas de disponibilidad ... 781
Disponibilidad por región ... 782
Administración de grupos de parámetros de clúster ... 784
Descripción de los grupos de parámetros de clúster ... 785
Creación de grupos de parámetros de clúster ... 792
Modificación de grupos de parámetros de clúster ... 795
Modificación de clústeres para utilizar grupos de parámetros de clúster personalizados ... 800
Copia de grupos de parámetros de clúster ... 801
Restablecimiento de los grupos de parámetros de clúster ... 804
Eliminación de grupos de parámetros de clúster ... 807
Referencia de parámetros de clúster ... 810
Descripción de puntos de conexión ... 833
Búsqueda de puntos de conexión de un clúster ... 834
Búsqueda del punto de conexión de una instancia ... 837
Conexión a puntos de conexión ... 840
Descripción de Amazon DocumentDB ARNs ... 842
Creación de un nombre ARN ... 842
Búsqueda de un ARN ... 846
Etiquetado de recursos ... 848
Información general de las etiquetas de recursos de ... 849
Restricciones de las etiquetas ... 850
Adición o actualización de etiquetas ... 850
Enumeración de etiquetas ... 852
Eliminación de etiquetas ... 853
Mantenimiento de Amazon DocumentDB ... 855
Notificaciones de parches del motor ... 856
Vista de mantenimiento pendiente ... 857
Actualizaciones del motor ... 859
Actualizaciones iniciadas por el usuario ... 863
Administración de los periodos de mantenimiento ... 864

Actualizaciones del sistema operativo 867
Descripción de los roles vinculados a servicios 870
Permisos de roles vinculados a servicios 871
Crear un rol vinculado a servicios 873
Modificación de un rol vinculado a servicios 873
Eliminar un rol vinculado a servicios 873
Regiones admitidas para los roles vinculados a servicios para Amazon DocumentDB 874
Uso de flujos de cambios 874
Operaciones admitidas 875
Facturación 876
Limitaciones 876
Habilitación de flujos de cambios 877
Uso de flujos de cambios con Python 879
Búsqueda completa de documentos 882
Reanudación de un flujo de cambios 882
Reanudación con `startAtOperationTime` 884
Reanudación con `postBatchResumeToken` 886
Transacciones 887
Modificación de la duración de la retención de registros 887
Flujos de cambios en instancias secundarias 891
Uso de la intercalación 892
Limitaciones 893
Uso de vistas 893
Prácticas recomendadas 894
Compatibilidad con los operadores de agregadores 895
Aprovechamiento de índices y vistas 895
Uso de AWS Lambda con flujos de cambios 895
Limitaciones 896
Uso de clústeres elásticos 898
Casos de uso de clústeres elásticos 899
Perfiles de usuario 899
Administración de contenido y registros históricos 899
Ventajas de los clústeres elásticos 899
AWS integración de servicios 899
Disponibilidad en regiones y versiones 900
Disponibilidad regional para clústeres elásticos 900

Disponibilidad de versiones ... 901
Limitaciones ... 901
Administración de clústeres elásticos ... 901
Operaciones de consulta y escritura ... 902
Gestión de colecciones e índices ... 902
Administración y diagnóstico ... 902
Características de suscripción ... 903
Cómo funcionan ... 903
Partición en los clústeres elásticos de Amazon DocumentDB ... 903
Migración de clústeres elásticos ... 907
Escalado de clústeres elásticos ... 907
Fiabilidad de los clústeres elásticos ... 907
Almacenamiento y disponibilidad de clústeres elásticos ... 907
Diferencias funcionales entre Amazon DocumentDB 4.0 y los clústeres elásticos ... 908
Introducción ... 909
Requisitos previos ... 910
Paso 1: crear un clúster elástico ... 911
Paso 2: conectarse a su clúster elástico ... 918
Paso 3: hacer una partición de su colección; insertar y consultar los datos ... 919
Paso 4: explorar ... 922
Prácticas recomendadas ... 923
Elección de las claves de partición ... 923
Administración de conexiones ... 923
Colecciones sin particiones ... 924
Escalado de clústeres elásticos ... 924
Monitoreo de clústeres elásticos ... 924
Administración de los clústeres elásticos ... 925
Modificación de configuraciones de clústeres elásticos ... 926
Monitoreo de un clúster elástico ... 929
Eliminación de un clúster elástico ... 933
Administración de instantáneas de los clústeres elásticos ... 935
Detención e inicio de un clúster elástico ... 950
Mantenimiento de clústeres elásticos ... 955
Cifrado de datos en reposo ... 963
Cómo utilizan las subvenciones los clústeres elásticos de Amazon DocumentDB en AWS KMS ... 965

Crear una clave administrada por el cliente ... 965
Supervisión de las claves de cifrado de clústeres elásticos de Amazon DocumentDB ... 967
Más información ... 972
Roles vinculados a servicios ... 973
Permisos de rol vinculado a servicios para clústeres elásticos ... 973
Monitorización de Amazon DocumentDB ... 978
Monitorización del estado de un clúster ... 979
Valores de estado del clúster ... 980
Monitorización del estado de un clúster ... 982
Monitorización del estado de una instancia ... 983
Valores de estado de instancia ... 984
Monitorear el estado de la instancia mediante Consola de administración de AWS o AWS CLI ... 987
Estado de una instancia ... 989
Supervisar el estado de la instancia mediante el Consola de administración de AWS ... 989
Visualización de recomendaciones de Amazon DocumentDB ... 991
Suscripciones de eventos ... 994
Suscripción a eventos ... 995
Administre las suscripciones ... 998
Categorías y mensajes ... 1002
Supervisión de Amazon DocumentDB con CloudWatch ... 1005
Métricas de Amazon DocumentDB ... 1006
Visualización CloudWatch de datos ... 1024
Dimensiones de Amazon DocumentDB ... 1030
Supervisión de métricas de Opcounter ... 1031
Supervisión de conexiones a bases de datos ... 1031
Registro de llamadas a la API de Amazon DocumentDB con CloudTrail ... 1031
Información de Amazon DocumentDB en CloudTrail ... 1032
Creación de perfiles de operaciones ... 1033
Operaciones admitidas ... 1034
Limitaciones ... 1034
Habilitación del generador de perfiles ... 1035
Deshabilitación del generador de perfiles ... 1039
Deshabilitación de la exportación de registros del generador de perfiles ... 1040
Acceso a los registros del generador de perfiles ... 1043
Consultas comunes ... 1043

Supervisión con información sobre rendimiento 1044
Conceptos de Información sobre rendimiento 1045
Activación y desactivación de Información sobre rendimiento 1049
Configuración de directivas de acceso para información sobre rendimiento 1053
Análisis de métricas mediante el panel de Información sobre rendimiento 1057
Recuperación de métricas con la API de Información sobre rendimiento 1078
CloudWatch Métricas de Amazon para Performance Insights 1093
Métricas de contador para Información sobre rendimiento 1096
OpenSearch integración 1098
Amazon OpenSearch Service como destino 1098
Paso 1: Crear un dominio de Amazon OpenSearch Service o una colección OpenSearch sin servidor 1099
Paso 2: habilitación de los flujos de cambios en el clúster de Amazon DocumentDB 1099
Paso 3: configuración del rol de canalización con permisos para escribir en el bucket de Amazon S3 y en el dominio o colección de destino 1099
Paso 4: agregación de los permisos necesarios en el rol de canalización para crear X-ENI 1100
Paso 5: creación de la canalización 1101
Limitaciones 1102
Uso de DocumentDB sin servidor 1103
Casos de uso de la tecnología sin servidor 1103
Uso de Amazon DocumentDB sin servidor para las cargas de trabajo aprovisionadas existentes 1105
Ventajas de Amazon DocumentDB sin servidor 1106
Cómo funciona sin servidor 1107
Descripción general de 1107
Configuraciones para clústeres de Amazon DocumentDB 1108
Capacidad de escalado de Amazon DocumentDB sin servidor 1109
Escalado de Amazon DocumentDB sin servidor 1111
Estado inactivo (0,5) DCUs 1113
Requisitos y limitaciones sin servidor 1114
Requisitos de características 1114
Limitaciones de características 1115
Creación de un clúster que utilice la tecnología sin servidor 1115
Creación de un clúster de Amazon DocumentDB sin servidor 1115
Añadido de una instancia de Amazon DocumentDB sin servidor 1118
Migración a sistemas sin servidor 1119

Migración de los clústeres de DocumentDB existentes a sistemas sin servidor 1119
Migración de MongoDB a DocumentDB sin servidor 1125
Administración sin sistemas sin servidor 1125
Visualización y modificación de la configuración del rango de capacidad de escalado de un clúster 1125
Visualización y modificación del nivel de promoción de los lectores sin servidor 1128
Límites de instancias sin servidor 1131
Configuración de escalado sin servidor 1133
Selección del rango de capacidad de escalado para un clúster de DocumentDB sin servidor 1133
Elección de la configuración `MinCapacity` para un clúster de DocumentDB sin servidor . 1134
Elección de la configuración `MaxCapacity` para un clúster de DocumentDB sin servidor . 1136
Evitar errores out-of-memory 1138
¿Por qué no se reduce verticalmente mi instancia sin servidor? 1139
Supervisión sin servidor 1140
Memoria insuficiente: estado de parámetros incompatibles 1140
CloudWatch Métricas de Amazon para DocumentDB sin servidor 1141
Supervisión del rendimiento de DocumentDB sin servidor con Información sobre rendimiento 1145
Desarrollo de Amazon DocumentDB 1147
Conexión a DocumentDB 1147
Conexión mediante programación 1147
Conexión desde fuera de una Amazon VPC 1176
Conexión como conjunto de réplicas 1178
Conexión mediante Studio 3T 1183
Conexión mediante DataGrip 1194
Connect mediante Amazon EC2 1202
Conexión mediante el controlador JDBC 1240
Conexión mediante el controlador ODBC 1258
Programación con DocumentDB 1274
Guía de programación de DocumentDB en Java 1274
Cómo utilizar la validación de esquemas JSON 1307
Cuotas y límites 1318
Tipos de instancias admitidas 1318
Regiones admitidas 1320
Cuotas regionales 1322

Límites de agregación ... 1325
Límites de los clústeres ... 1325
Límites de instancias ... 1327
Restricciones en la nomenclatura ... 1330
Restricciones de TTL ... 1332
Límites de clústeres elásticos ... 1332
Límites de partición de clústeres elásticos ... 1333
Límites de CPU, memoria, conexión y cursor de los clústeres elásticos por partición ... 1333
Consultas ... 1335
Consulta de documentos ... 1335
Recuperación de todos los documentos ... 1336
Valores de campo coincidentes ... 1336
Documentos incrustados ... 1336
Valores de campo en documentos incrustados ... 1337
Coincidencia de una matriz ... 1337
Valores coincidentes en una matriz ... 1337
Uso de operadores ... 1338
Plan de consulta ... 1338
Plan de consulta ... 1338
Memoria caché de planes de consultas ... 1340
Descripción de los resultados ... 1340
Etapa de escaneo y filtrado ... 1341
Intersección de índices ... 1342
Unión de índices ... 1343
Intersección/unión de índices múltiples ... 1344
Índice compuesto ... 1344
Etapa de clasificación ... 1345
Etapa de grupos ... 1345
Planificador de consultas v2 ... 1345
Requisitos previos ... 1346
Selección de la versión 2.0 del planificador como planificador de consultas predeterminado ... 1346
Prácticas recomendadas ... 1347
Limitaciones ... 1347
Mejoras en operadores `Find` y `Update` ... 1347
API del filtro de caché del plan ... 1351

Posibles diferencias de comportamiento entre el planificador, versión 1.0, 2.0 y MongoDB 1353
La versión 2.0 del planificador cierra la brecha de comportamiento con MongoDB 1360
Planificador de consultas v3 1362
Requisitos previos 1346
Seleccionar la versión 3.0 del planificador como planificador de consultas predeterminado 1346
Prácticas recomendadas 1347
Limitaciones 1347
Mejoras en operadores `aggregate` y `distinct` 1347
Posibles diferencias de comportamiento entre las versiones 1.0, 3.0 y MongoDB del planificador 1353
Datos geoespaciales 1367
Descripción general de 1
Indexación y almacenamiento de datos geoespaciales 1367
Consulta de datos geoespaciales 1369
Limitaciones 1373
Índice parcial 1373
Creación de un índice parcial 1374
Operadores admitidos 1374
Consulta mediante un índice parcial 1374
Funcionalidades de indexación parcial 1375
Limitaciones del índice parcial 1379
Búsqueda de texto 1381
Funcionalidades admitidas 1381
Uso del índice de texto de Amazon DocumentDB 1381
Diferencias con MongoDB 1387
Prácticas recomendadas y directrices 1388
Índice de texto V2 1388
Limitaciones 1389
Solución de problemas 1390
Problemas de conectividad 1390
No se puede conectar a un punto de conexión de Amazon DocumentDB 1390
Comprobación de una conexión a una instancia de Amazon DocumentDB 1396
Conexión a un punto de conexión no válido 1396
La configuración del controlador afecta al número de conexiones 1397
Índices 1397
Error al crear un índice 1398

El índice en segundo plano genera problemas de latencia y falla 1398
Sobrecarga del índice 1399
Rendimiento y utilización de recursos 1400
Consulta las estadísticas de inserción, actualización y eliminación 1401
Análisis del rendimiento de la memoria caché 1402
Encontrar y terminar las consultas que tardan mucho en ejecutarse o se bloquean 1404
Ver un plan de consultas y optimizar una consulta 1405
¿Cómo puedo ver un plan de consultas en clústeres elásticos? 1407
Ver todas las operaciones en ejecución en una instancia 1410
Saber cuándo una consulta está avanzando 1412
Determinar por qué de repente un sistema se ejecuta lentamente 1415
Determinar la causa del uso elevado de la CPU 1417
Búsqueda de los cursores abiertos en una instancia 1418
Visualización de la versión actual del motor Amazon DocumentDB 1418
Análisis del uso de los índices e identificar los índices no utilizados 1419
Identificación de los índices omitidos 1421
¿Cómo determino la sobrecarga de colecciones de bases de datos? 1423
Resumen de consultas útiles 1424
Recopilación de elementos no utilizados 1425
Descripción de la recolección de basura en Amazon DocumentDB 1426
Proceso de recopilación de elementos no utilizados 1426
Arquitectura de almacenamiento y almacenamiento ampliado 1427
Supervisión de recopilación de elementos no utilizados 1428
Ejemplo de salida de CollStats 1431
Preguntas frecuentes 1433
Referencia de la API para la administración de recursos 1437
Acciones 1437
Amazon DocumentDB (with MongoDB compatibility) 1440
Amazon DocumentDB Elastic Clusters 1634
Data Types 1722
Amazon DocumentDB (with MongoDB compatibility) 1724
Amazon DocumentDB Elastic Clusters 1810
Errores comunes 1829
Parámetros comunes 1830
Notas de la versión 1834
08 de enero de 2026 1837

Nueva característica 1837
11 de noviembre de 2025 1837
Nuevas características 1837
22 de octubre de 2025 1838
Nuevas características 1838
16 de octubre de 2025 1838
Nueva característica 1838
13 de octubre de 2025 1839
Nueva característica 1839
7 de octubre de 2025 1839
Nueva característica 1839
26 de septiembre de 2025 1839
Nuevas características 1839
15 de septiembre de 2025 1840
Correcciones de errores y otros cambios 1840
29 de julio de 2025 1840
Nuevas características 1840
Correcciones de errores y otros cambios 1841
28 de julio de 2025 1841
Nuevas características 1841
18 de junio de 2025 1841
Nueva característica 1841
8 de mayo de 2025 1841
Nueva característica 1841
2 de abril de 2025 1842
Correcciones de errores y otros cambios 1842
24 de marzo de 2025 1842
Nueva característica 1842
6 de febrero de 2025 1842
Nueva característica 1842
28 de enero de 2025 1842
Nueva característica 1842
15 de enero de 2025 1843
Nuevas características 1843
Correcciones de errores y otros cambios 1843
18 de diciembre de 2024 1843

Nuevas características 1843
12 de noviembre de 2024 1844
Nuevas características 1844
6 de noviembre de 2024 1844
Nuevas características 1844
1 de noviembre de 2024 1844
Nueva característica 1844
22 de octubre de 2024 1844
Nueva característica 1844
18 de septiembre de 2024 1845
Nueva característica 1845
17 de septiembre de 2024 1845
Nuevas características 1845
Correcciones de errores y otros cambios 1845
22 de agosto de 2024 1846
Nueva característica 1846
20 de agosto de 2024 1846
Nueva característica 1846
8 de agosto de 2024 1846
Nueva característica 1846
23 de julio de 2024 1847
Nuevas características 1847
Correcciones de errores y otros cambios 1848
22 de julio de 2024 1848
Nuevas características 1848
Correcciones de errores y otros cambios 1849
9 de julio de 2024 1849
Nueva característica 1849
8 de julio de 2024 1849
Nueva característica 1849
25 de junio de 2024 1850
Nueva característica 1850
29 de mayo de 2024 1850
Nuevas características 1850
3 de abril de 2024 1850
Nuevas características 1850

Correcciones de errores y otros cambios 1851
22 de febrero de 2024 1851
Nuevas características 1851
30 de enero de 2024 1852
Nuevas características 1852
10 de enero de 2024 1852
Nuevas características 1852
Correcciones de errores y otros cambios 1854
20 de diciembre de 2023 1854
Otros cambios 1854
13 de diciembre de 2023 1854
Nuevas características 1854
29 de noviembre de 2023 1854
Nuevas características 1854
21 de noviembre de 2023 1855
Nuevas características 1855
17 de noviembre de 2023 1855
Nuevas características 1855
Correcciones de errores y otros cambios 1855
6 de noviembre de 2023 1855
Nuevas características 1855
Correcciones de errores y otros cambios 1856
25 de septiembre de 2023 1856
Nuevas características 1856
20 de septiembre de 2023 1856
Nuevas características 1856
15 de septiembre de 2023 1856
Nuevas características 1856
11 de septiembre de 2023 1857
Nuevas características 1857
3 de agosto de 2023 1857
Nuevas características 1857
13 de julio de 2023 1857
Nuevas características 1857
Correcciones de errores y otros cambios 1858
7 de junio de 2023 1858

Correcciones de errores y otros cambios 1858
10 de mayo de 2023 1858
Correcciones de errores y otros cambios 1858
4 de abril de 2023 1859
Correcciones de errores y otros cambios 1859
22 de marzo de 2023 1859
Nuevas características 1859
1 de marzo de 2023 1860
Nuevas características 1860
27 de febrero de 2023 1860
Correcciones de errores y otros cambios 1860
2 de febrero de 2023 1861
Correcciones de errores y otros cambios 1861
30 de noviembre de 2022 1861
Nuevas características 1861
9 de agosto de 2022 1861
Nuevas características 1861
Correcciones de errores y otros cambios 1862
25 de julio de 2022 1862
Nuevas características 1862
27 de junio de 2022 1862
Nuevas características 1862
29 de abril de 2022 1863
Nuevas características 1863
7 de abril de 2022 1863
Nuevas características 1863
16 de marzo de 2022 1863
Nuevas características 1863
8 de febrero de 2022 1863
Nuevas características 1863
24 de enero de 2022 1863
Nuevas características 1863
21 de enero de 2022 1864
Nuevas características 1864
25 de octubre de 2021 1865
Nuevas características 1865

Correcciones de errores y otros cambios 1865
24 de junio de 2021 1866
Nuevas características 1866
4 de mayo de 2021 1866
Nuevas características 1866
Correcciones de errores y otros cambios 1867
15 de enero de 2021 1867
Nuevas características 1867
9 de noviembre de 2020 1868
Nuevas características 1868
Correcciones de errores y otros cambios 1869
30 de octubre de 2020 1870
Nuevas características 1870
Correcciones de errores y otros cambios 1870
22 de septiembre de 2020 1871
Nuevas características 1871
Correcciones de errores y otros cambios 1871
10 de julio de 2020 1871
Nuevas características 1871
Correcciones de errores y otros cambios 1871
30 de junio de 2020 1871
Nuevas características 1871
Correcciones de errores y otros cambios 1872
Historial de revisión 1873
..... mdccclxxxv

Qué es Amazon DocumentDB (compatible con MongoDB)

Amazon DocumentDB (compatible con MongoDB) es un servicio rápido, de confianza y completamente administrado. Amazon DocumentDB simplifica la configuración, la administración y el escalado de bases de datos compatibles con MongoDB en la nube. Con Amazon DocumentDB, puede ejecutar el mismo código de aplicación y utilizar los mismos controladores y herramientas que utiliza con MongoDB.

Antes de utilizar Amazon DocumentDB, debe revisar los conceptos y las características que se describen en Cómo funcionan. A continuación, realice los pasos que se indican en Guía de introducción.

Temas

- Información general de Amazon DocumentDB
- Clústeres
- instancias
- Regiones y zonas de disponibilidad
- Precios de Amazon DocumentDB
- Supervisión
- Interfaces
- Siguientes pasos
- Funcionamiento de Amazon DocumentDB
- ¿Qué es una base de datos de documentos?

Información general de Amazon DocumentDB

A continuación, se muestran algunas de las características generales de Amazon DocumentDB:

- Amazon DocumentDB admite dos tipos de clústeres: clústeres basados en instancias y clústeres elásticos. Los clústeres elásticos admiten cargas de trabajo con una capacidad de reads/writes almacenamiento de millones por segundo y petabytes. Para obtener más información acerca de los clústeres elásticos, consulte Uso de Amazon DocumentDB Elastic Clusters. El siguiente contenido hace referencia a los clústeres basados en instancias de Amazon DocumentDB.

- Amazon DocumentDB aumenta automáticamente el tamaño del volumen de almacenamiento a medida que aumentan las necesidades de almacenamiento de la base de datos. El volumen de almacenamiento aumenta en incrementos de 10 GB, hasta un máximo de 128 TiB. No necesita aprovisionar almacenamiento excesivo para el clúster a fin de afrontar el crecimiento en el futuro.
- Con Amazon DocumentDB, puede aumentar el rendimiento de lectura para admitir solicitudes de aplicaciones de gran volumen mediante la creación de hasta 15 instancias de réplica. Las réplicas de Amazon DocumentDB comparten el mismo almacenamiento subyacente, lo que reduce los costos y evita la necesidad de realizar escrituras en los nodos de réplica. Esta capacidad libera más potencia de procesamiento para atender las solicitudes de lectura y reduce el tiempo de retraso de la réplica, que a menudo se reduce a milisegundos de un solo dígito. Puede añadir réplicas en cuestión de minutos, independientemente del tamaño del volumen de almacenamiento. Amazon DocumentDB también proporciona un punto de conexión de lectura para que la aplicación pueda conectarse sin tener que realizar un seguimiento de las réplicas a medida que se añaden o quitan.
- Amazon DocumentDB le permite escalar los recursos informáticos y memoria para cada una de las instancias. Las operaciones de escalado de los recursos informáticos normalmente se llevan a cabo en cuestión de minutos.
- Amazon DocumentDB se ejecuta en Amazon Virtual Private Cloud (Amazon VPC), de modo que puede aislar su base de datos en su propia red virtual. También puede configurar ajustes del firewall para controlar el acceso de red al clúster.
- Amazon DocumentDB monitoriza continuamente el estado del clúster. Si se produce un error en una instancia, Amazon DocumentDB reinicia automáticamente la instancia y los procesos asociados. Amazon DocumentDB no requiere una reproducción de los reregistros de la base de datos durante la recuperación tras un bloqueo, lo que reduce considerablemente los tiempos de reinicio. Amazon DocumentDB también aísla la caché de la base de datos del proceso de la base de datos, lo que permite que la caché sobreviva a un reinicio de la instancia.
- Cuando ocurre un error en una instancia, Amazon DocumentDB automatiza la conmutación por error en una de las 15 réplicas de Amazon DocumentDB que crea en otras zonas de disponibilidad. Si no se han aprovisionado réplicas y se produce un error, Amazon DocumentDB intenta crear una nueva instancia de Amazon DocumentDB de forma automática.
- La capacidad de copia de seguridad de Amazon DocumentDB permite point-in-time la recuperación del clúster. Esta característica le permite restaurar el clúster a cualquier segundo dentro de su período de retención, hasta los últimos 5 minutos. Puede configurar el período de retención de copia de seguridad automático hasta un máximo de 35 días. Las copias de seguridad automatizadas se almacenan en Amazon Simple Storage Service (Amazon S3), diseñado para

una durabilidad del 99,999999999 %. Las copias de seguridad de Amazon DocumentDB son automáticas, incrementales y continuas, y no afectan al rendimiento del clúster.

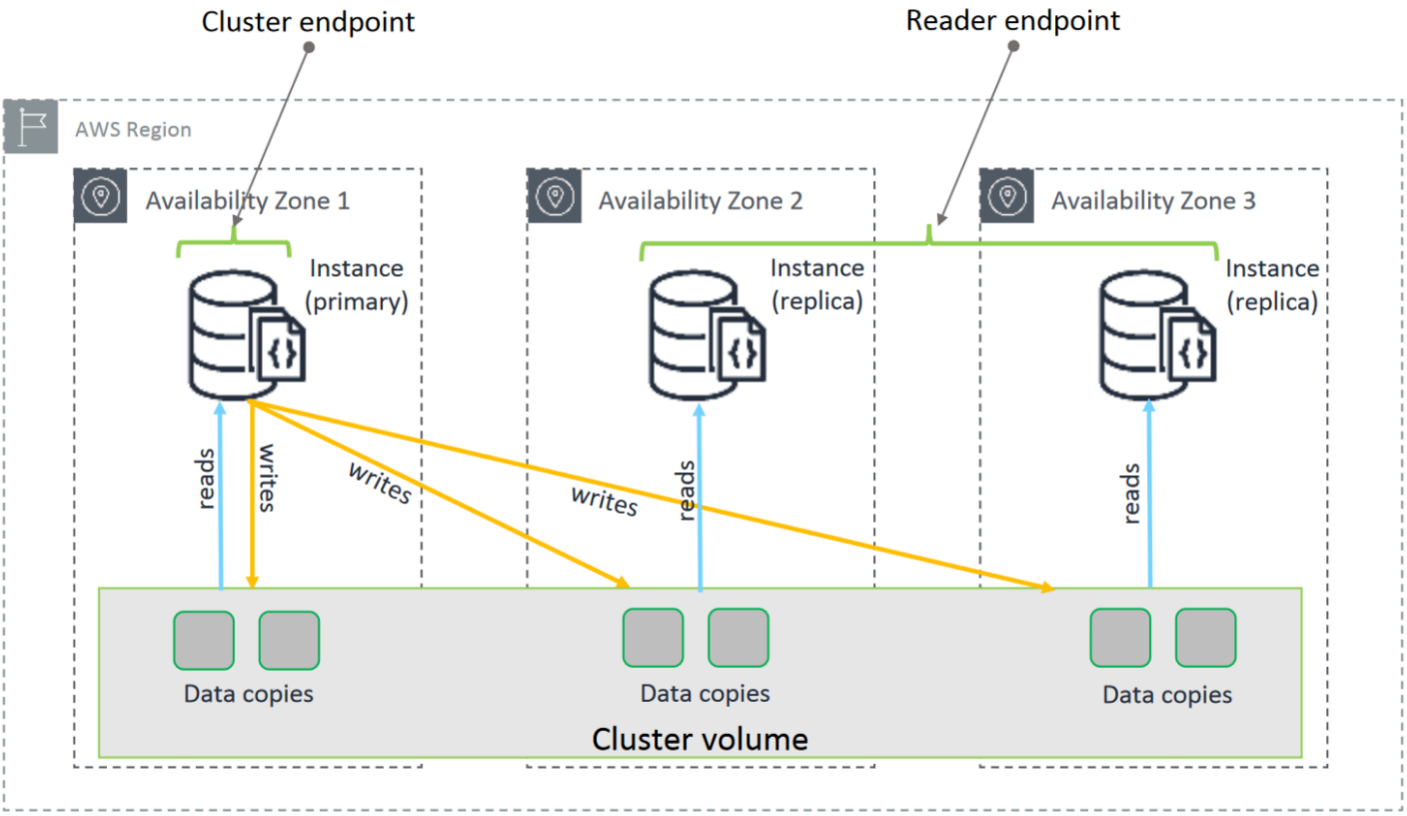
- Con Amazon DocumentDB, puede cifrar sus bases de datos mediante claves que cree y controle mediante AWS Key Management Service ().AWS KMS En un clúster de base de datos que se ejecute con el cifrado de Amazon DocumentDB, los datos almacenados en reposo en el almacenamiento subyacente están cifrados. Las copias de seguridad automatizadas, las instantáneas y las réplicas que se encuentran en el mismo clúster también están cifradas.
- Amazon DocumentDB está autorizada por el Programa federal de administración de riesgos y autorizaciones (FedRAMP). Cuenta con una autorización alta de FedRAMP AWS GovCloud para las regiones (EE. UU.) y una autorización moderada de FedRAMP para las regiones de EE. UU. AWS East/West Para obtener información detallada AWS y sobre las iniciativas de cumplimiento, consulte los AWS servicios incluidos en el ámbito de aplicación por programa de cumplimiento.

Si es la primera vez que utiliza AWS los servicios, utilice los siguientes recursos para obtener más información:

- AWS ofrece servicios de informática, bases de datos, almacenamiento, análisis y otras funciones. Para obtener una descripción general de todos los AWS servicios, consulte Computación en la nube con Amazon Web Services.
- AWS proporciona una serie de servicios de bases de datos. Para averiguar cuál es el mejor servicio para su entorno, consulte Bases de datos en AWS.

Clústeres

Un clúster contiene entre 0 y 16 instancias y un volumen de almacenamiento del clúster que administra los datos de esas instancias. Todos los procesos de escritura se efectúan a través de la instancia principal. Todas las instancias (principales y réplicas) admiten operaciones de lectura. Los datos del clúster se almacenan en el volumen del clúster con copias en tres zonas de disponibilidad diferentes.



Los clústeres basados en instancias de Amazon DocumentDB 5.0 admiten dos configuraciones de almacenamiento para un clúster de base de datos: Amazon DocumentDB estándar y Amazon DocumentDB optimizado para E/S. Para obtener más información, consulte Configuraciones de almacenamiento en clústeres de Amazon DocumentDB.

instancias

Una instancia de Amazon DocumentDB es un entorno de base de datos aislado en la nube. Una instancia puede contener varias bases de datos creadas por el usuario. Puede crear y modificar una instancia mediante el Consola de administración de AWS o el AWS CLI.

La capacidad de computación y de memoria de una instancia se determina mediante su clase de instancia. Puede seleccionar la instancia que mejor se adapte a sus necesidades. Si sus necesidades cambian con el tiempo, puede elegir otra clase de instancia. Para ver las especificaciones de las clases de instancias, consulte Especificaciones de clases de instancias.

Las instancias de Amazon DocumentDB se ejecutan únicamente en el entorno de Amazon VPC. Amazon VPC le permite controlar su entorno de red virtual: puede elegir su propio rango de direcciones IP, crear subredes y configurar listas de enrutamiento y control de acceso (). ACLs

Antes de crear instancias de Amazon DocumentDB, debe crear un clúster que contenga las instancias.

Todas las clases de instancias no se admiten en todas las regiones. En la tabla siguiente, se muestran las clases de instancias que admite cada región.

> **Note**
>
> Para ver una lista completa de tipos de instancias compatibles con Amazon DocumentDB en cada clase de instancias, consulte Especificaciones de clases de instancias.

Clases de instancias admitidas por región

Region	R8G	R6GD	R6G	R5	R4	T4G	T3	Sin servidor
Este de EE. UU. (Ohio)	Soportado	Soportado	Soportado	Soportado	Soportado	Soportado	Soportado	compatible
Este de EE. UU. (Norte de Virginia)	Soportado	Soportado	Soportado	Soportado	Soportado	Soportado	Soportado	compatible
Oeste de EE. UU. (Oregón)	Soportado	Soportado	Soportado	Soportado	Soportado	Soportado	Soportado	compatible
África (Ciudad del Cabo)			Soportado	Soportado		Soportado	Soportado	compatible
América del Sur (São Paulo)		Soportado	Soportado	Soportado		Soportado	Soportado	compatible
Asia-Pacífico (Hong Kong)			Soportado	Soportado		Soportado	Soportado	compatible
Asia-Pacífico (Hyderabad)			Soportado	Soportado		Soportado	Soportado	compatible

Region	R8G	R6GD	R6G	R5	R4	T4G	T3	Sin servidor
Asia-Pacífico (Malasia)			Soportado			Soportado	compatible	
Asia-Pacífico (Mumbai)	Soportado	Soportado	Soportado	Soportado		Soportado	Soportado	compatible
Asia-Pacífico (Osaka)		Soportado	Soportado	Soportado		Soportado	compatible	
Asia-Pacífico (Seúl)	Soportado	Soportado	Soportado	Soportado		Soportado	Soportado	compatible
Asia-Pacífico (Sídney)	Soportado	Soportado	Soportado	Soportado		Soportado	Soportado	compatible
Asia-Pacífico (Yakarta)	Soportado	Soportado	Soportado	Soportado		Soportado	compatible	
Asia-Pacífico (Singapur)	Soportado	Soportado	Soportado	Soportado		Soportado	Soportado	compatible
Asia-Pacífico (Tailandia)			Soportado			Soportado	compatible	
Asia-Pacífico (Tokio)	Soportado	Soportado	Soportado	Soportado		Soportado	Soportado	compatible
Canadá (centro)		Soportado	Soportado	Soportado		Soportado	Soportado	compatible
Europa (Fráncfort)	Soportado	Soportado	Soportado	Soportado		Soportado	Soportado	compatible
Europa (Irlanda)	Soportado	Soportado	Soportado	Soportado	Soportado	Soportado	Soportado	compatible

Region	R8G	R6GD	R6G	R5	R4	T4G	T3	Sin servidor
Europa (Londres)		Soportado	Soportado	Soportado		Soportado	Soportado	compatible
Europa (Milán)			Soportado	Soportado		Soportado	Soportado	compatible
Europa (París)		Soportado	Soportado	Soportado		Soportado	Soportado	compatible
Europa (España)	Soportado	Soportado	Soportado	Soportado		Soportado	Soportado	compatible
Europa (Estocolmo)	Soportado	Soportado	Soportado	Soportado		Soportado	compatible	
México (centro)			Soportado			Soportado	compatible	
Medio Oriente (EAU)			Soportado	Soportado		Soportado	Soportado	compatible
China (Pekín)		Soportado	Soportado	Soportado		Soportado	Soportado	compatible
China (Ningxia)			Soportado	Soportado		Soportado	Soportado	compatible
Israel (Tel Aviv)			Soportado	Soportado		Soportado	Soportado	compatible
AWS GovCloud (EE. UU.-Oeste)	Soportado	Soportado	Soportado	Soportado		Soportado	Soportado	compatible
AWS GovCloud (EE. UU.-Este)		Soportado	Soportado	Soportado		Soportado	Soportado	compatible

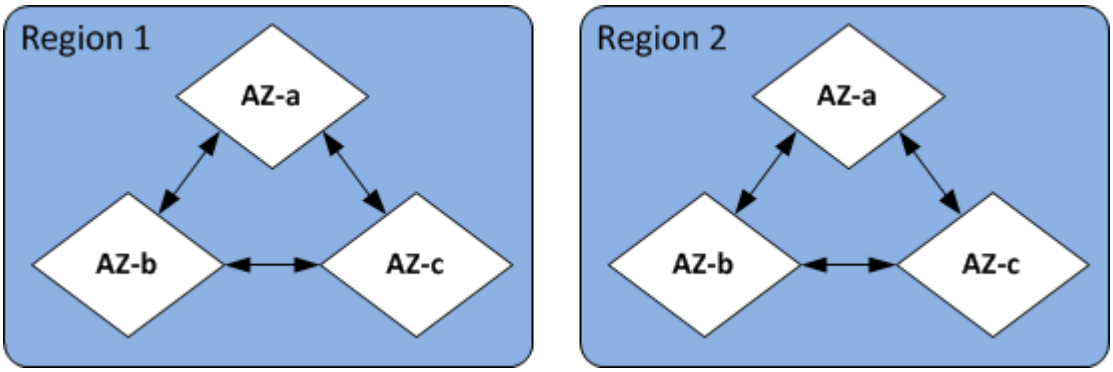
Regiones y zonas de disponibilidad

Las regiones y las zonas de disponibilidad definen las ubicaciones físicas del clúster y de las instancias.

Regions

AWS Los recursos de computación en la nube se encuentran en instalaciones de centros de datos de alta disponibilidad en diferentes áreas del mundo (por ejemplo, América del Norte, Europa o Asia). Cada ubicación de centro de datos se denomina región.

Cada AWS región está diseñada para estar completamente aislada de las demás AWS regiones. Dentro de cada una de ellas hay varias zonas de disponibilidad. Al lanzar los nodos en zonas de disponibilidad diferentes, puede lograr la máxima tolerancia a errores. El siguiente diagrama muestra una vista general del funcionamiento de AWS las regiones y las zonas de disponibilidad.



Zonas de disponibilidad

Cada AWS región contiene varias ubicaciones distintas denominadas zonas de disponibilidad. Cada zona de disponibilidad está diseñada para estar aislada de los errores que se produzcan en otras zonas de disponibilidad y para proporcionar conectividad de red de baja latencia económica con otras zonas de disponibilidad de la misma región. Al lanzar instancias para un clúster determinado en varias zonas de disponibilidad, puede proteger las aplicaciones en el caso improbable de que se produzca un error en una zona de disponibilidad.

La arquitectura de Amazon DocumentDB separa el almacenamiento y la computación. Para la capa de almacenamiento, Amazon DocumentDB replica seis copias de los datos en tres AWS zonas de disponibilidad. Por ejemplo, si lanza un clúster de Amazon DocumentDB en una región que solo admite dos zonas de disponibilidad, el almacenamiento de datos se replicará de seis maneras en tres zonas de disponibilidad, pero las instancias de computación solo estarán disponibles en dos zonas de disponibilidad.

En la siguiente tabla, se indica el número de zonas de disponibilidad que puede utilizar en una determinada zona Región de AWS para aprovisionar instancias informáticas para su clúster.

Nombre de la región	Region	Zonas de disponibilidad (cálculo)
Este de EE. UU. (Ohio)	`us-east-2`	3
Este de EE. UU. (Norte de Virginia)	`us-east-1`	6
Oeste de EE. UU. (Oregón)	`us-west-2`	4
África (Ciudad del Cabo)	`af-south-1`	3
América del Sur (São Paulo)	`sa-east-1`	3
Asia-Pacífico (Hong Kong)	`ap-east-1`	3
Asia-Pacífico (Hyderabad)	`ap-south-2`	3
Asia-Pacífico (Malasia)	`ap-southeast-5`	3
Asia-Pacífico (Mumbai)	`ap-south-1`	3
Asia-Pacífico (Osaka)	`ap-northeast-3`	3
Asia-Pacífico (Seúl)	`ap-northeast-2`	4
Asia-Pacífico (Singapur)	`ap-southeast-1`	3
Asia-Pacífico (Sídney)	`ap-southeast-2`	3

Nombre de la región	Region	Zonas de disponibilidad (cálculo)
Asia-Pacífico (Yakarta)	ap-southeast-3	3
Asia-Pacífico (Tailandia)	ap-southeast-7	3
Asia-Pacífico (Tokio)	ap-northeast-1	3
Canadá (centro)	ca-central-1	3
Región China (Pekín)	cn-north-1	3
China (Ningxia)	cn-northwest-1	3
Europa (Fráncfort)	eu-central-1	3
Europa (Irlanda)	eu-west-1	3
Europa (Londres)	eu-west-2	3
Europa (Milán)	eu-south-1	3
Europa (París)	eu-west-3	3
Europa (España)	eu-south-2	3
Europa (Estocolmo)	eu-north-1	3
México (centro)	mx-central-1	3
Medio Oriente (EAU)	me-central-1	3
Israel (Tel Aviv)	il-central-1	3
AWS GovCloud (EE. UU.-Oeste)	us-gov-west-1	3
AWS GovCloud (EE. UU.-Este)	us-gov-east-1	3

Precios de Amazon DocumentDB

Los clústeres de Amazon DocumentDB se facturan en función de los siguientes componentes:

- Horas de instancia (por hora): en función de la clase de instancia (por ejemplo,`db.r5.xlarge`). Los precios se muestran por hora, pero las facturas se ajustan hasta el segundo y muestran las horas en formato decimal. El uso de Amazon DocumentDB se factura por incrementos de un segundo, con un mínimo de 10 minutos. Para obtener más información, consulte Administración de clases de instancias.
- Solicitudes de E/S (por cada millón de solicitudes al mes): número total de I/O solicitudes de almacenamiento que realiza en un ciclo de facturación.
- Almacenamiento de copias de seguridad (por GiB al mes): el almacenamiento de copias de seguridad es el almacenamiento asociado a copias de seguridad de base de datos automatizadas que haya realizado. Aumentar el período de retención de copia de seguridad u obtener instantáneas de base de datos adicionales aumenta el almacenamiento de copias de seguridad consumido por su base de datos. El almacenamiento de copias de seguridad se mide en GB-meses y no se aplica la tarificación por segundos. Para obtener más información, consulte Copia de seguridad y restauración en Amazon DocumentDB.
- Transferencia de datos (por GB): transferencia de datos de entrada y salida de la instancia desde o hacia Internet u otras AWS regiones.

Para obtener información detallada, consulte los precios de Amazon DocumentDB.

Prueba gratuita

Puede probar Amazon DocumentDB de forma gratuita con la versión de prueba gratuita de 1 mes. Para obtener más información, consulte los precios de la prueba gratuita en Amazon DocumentDB o consulte las preguntas frecuentes sobre la prueba gratuita de Amazon DocumentDB.

Supervisión

Hay varias formas de hacer un seguimiento del rendimiento y el estado de una instancia. Puedes usar el CloudWatch servicio gratuito de Amazon para supervisar el rendimiento y el estado de una instancia. Puede encontrar gráficos de rendimiento en la consola de Amazon DocumentDB. Puede suscribirse a eventos de Amazon DocumentDB si desea recibir una notificación cuando se produzcan cambios en una instancia, una instantánea, un grupo de parámetros o un grupo de seguridad.

Para obtener más información, consulte los siguientes temas:

- Supervisión de Amazon DocumentDB con CloudWatch
- Registro de llamadas a la API de Amazon DocumentDB con AWS CloudTrail

Interfaces

Existen varias formas de interactuar con Amazon DocumentDB, incluidas la Consola de administración de AWS y la. AWS CLI

Consola de administración de AWS

Consola de administración de AWS Se trata de una sencilla interfaz de usuario basada en la web. Desde la consola puede administrar sus clústeres e instancias sin necesidad de programación. Para acceder a la consola de Amazon DocumentDB, inicie sesión en Consola de administración de AWS y abra la consola de Amazon DocumentDB en /docdb. https://console.aws.amazon.com

AWS CLI

Puede usar AWS Command Line Interface (AWS CLI) para administrar sus instancias y clústeres de Amazon DocumentDB. Con una configuración mínima, puede comenzar a utilizar toda la funcionalidad que ofrece la consola de Amazon DocumentDB con el programa de terminal que desee.

- Para instalar el AWS CLI, consulte Instalación de la interfaz de línea de AWS comandos.
- Para empezar a utilizar Amazon DocumentDB, consulte la AWS CLI referencia de la interfaz de línea de AWS comandos de Amazon DocumentDB.

Controladores de MongoDB

Para desarrollar y escribir aplicaciones en un clúster de Amazon DocumentDB, también puede utilizar los controladores de MongoDB con Amazon DocumentDB. Para obtener más información, consulte la pestaña del intérprete de comandos de MongoDB en Conexión con TLS habilitado o Conexión con TLS deshabilitado.

Siguientes pasos

En la sección anterior se han presentado los componentes de la infraestructura básica ofrecidos por Amazon DocumentDB. ¿Qué debería hacer a continuación? Dependiendo de sus circunstancias, consulte uno de los siguientes temas para empezar.

- Comience a utilizar Amazon DocumentDB creando un clúster y una instancia mediante. CloudFormation Inicio rápido de Amazon DocumentDB con CloudFormation
- Empiece a trabajar con Amazon DocumentDB creando un clúster y una instancia con las instrucciones que se proporcionan en nuestro Guía de introducción.
- Comience a utilizar Amazon DocumentDB creando un clúster elástico siguiendo las instrucciones que se indican en Introducción a los clústeres elásticos de Amazon DocumentDB.
- Migre su implementación de MongoDB a Amazon DocumentDB utilizando las instrucciones en Migración a Amazon DocumentDB

Funcionamiento de Amazon DocumentDB

Amazon DocumentDB (compatible con MongoDB) es un servicio de base de datos completamente administrado y compatible con MongoDB. Con Amazon DocumentDB, puede ejecutar el mismo código de aplicación y utilizar los mismos controladores y herramientas que utiliza con MongoDB. Amazon DocumentDB es compatible con MongoDB 3.6, 4.0 y 5.0.

Temas

- Puntos de conexión de Amazon DocumentDB
- Compatibilidad con TLS
- Almacenamiento de Amazon DocumentDB
- Replicación de Amazon DocumentDB
- Fiabilidad de Amazon DocumentDB
- Opciones de preferencia de lectura
- Eliminaciones de TTL
- Recursos facturables

Cuando utilice Amazon DocumentDB, empezará creando un clúster. Un clúster se compone de cero o varias instancias y de un volumen de clúster que administra los datos de esas instancias. Un

volumen de clúster de Amazon DocumentDB es un volumen de almacenamiento de base de datos virtual que abarca varias zonas de disponibilidad. Cada zona de disponibilidad tiene una copia de los datos del clúster.

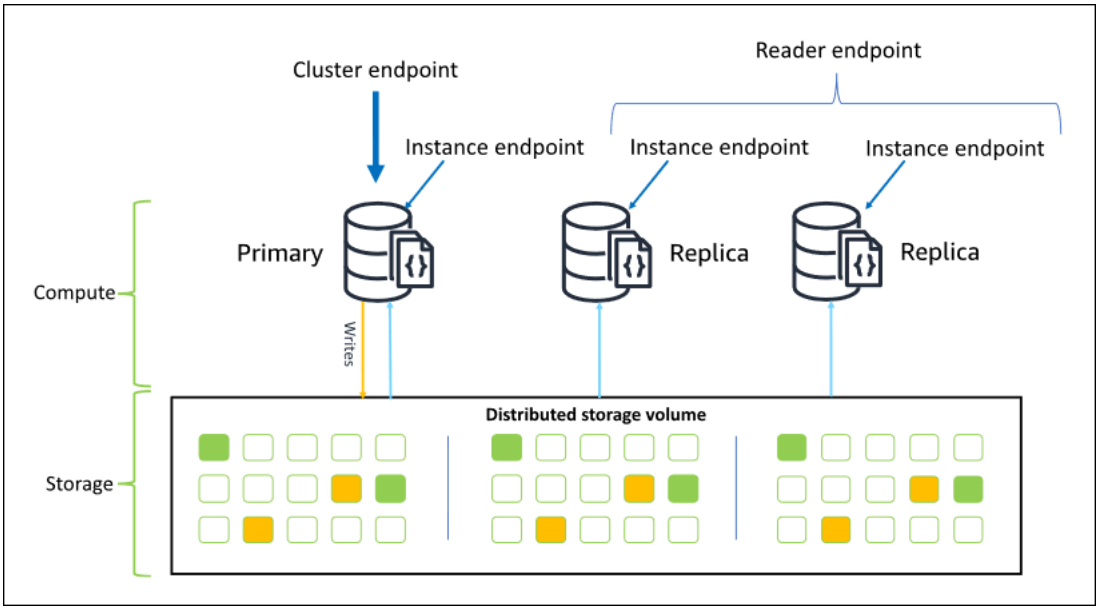
Los clústeres de Amazon DocumentDB constan de dos componentes principales:

- Volumen de clúster: utiliza un servicio de almacenamiento nativo en la nube para replicar los datos de seis maneras en tres zonas de disponibilidad, lo que proporciona un almacenamiento disponible y duradero. Un clúster de Amazon DocumentDB tiene exactamente un volumen de clúster, que puede almacenar hasta 128 TiB de datos.
- Instancias: proporcionan la potencia de procesamiento de la base de datos al escribir y leer datos desde el volumen de almacenamiento del clúster. Un clúster de Amazon DocumentDB puede tener de 0 a 16 instancias.

Las instancias adoptan uno de estos dos roles:

- Instancia de base de datos principal: admite operaciones de lectura y escritura y realiza todas las modificaciones de los datos en el volumen de clúster. Cada clúster de Amazon DocumentDB tiene una instancia principal.
- Instancia de réplica: solo admite operaciones de lectura. Un clúster de Amazon DocumentDB puede tener hasta 15 réplicas, además de la instancia principal. El hecho de disponer de varias réplicas le permite distribuir las cargas de trabajo de lectura. Además, al colocar las réplicas en distintas zonas de disponibilidad, también puede aumentar la disponibilidad del clúster.

En el siguiente diagrama se ilustra la relación entre el volumen de clúster, la instancia principal y las réplicas de un clúster de Amazon DocumentDB:



Las instancias del clúster no tienen por qué ser de la misma clase, y se pueden aprovisionar y terminar según sea necesario. Esta arquitectura le permite escalar la capacidad de cómputo de su clúster de forma independiente de su almacenamiento.

Cuando la aplicación escribe datos en la instancia principal, la instancia principal ejecuta una operación de escritura duradera en el volumen del clúster. A continuación, replica el estado de esa escritura (no los datos) en cada réplica activa. Las réplicas de Amazon DocumentDB no participan en el procesamiento de escrituras y, por lo tanto, las réplicas de Amazon DocumentDB son ventajosas para el escalado de lectura. Las lecturas de réplicas de Amazon DocumentDB son, en última instancia, consistentes con un retardo de réplica mínimo, normalmente menos de 100 milisegundos una vez que la instancia principal escribe los datos. Se garantiza que las operaciones de lectura de las réplicas se realizan en el orden en que fueron escritas en la instancia principal. El retardo de la réplica varía en función de la frecuencia de cambio de datos, y los periodos con mucha actividad de escritura pueden aumentar el retardo de la réplica. Para obtener más información, consulte las métricas `ReplicationLag` en Métricas de Amazon DocumentDB.

Puntos de conexión de Amazon DocumentDB

Amazon DocumentDB ofrece varias opciones de conexión para proporcionar una amplia variedad de casos de uso. Para conectarse a una instancia de un clúster de Amazon DocumentDB, debe especificar el punto de conexión de la instancia. Un punto de conexión es una dirección y un número de puerto de host, separados por dos puntos.

Le recomendamos que se conecte al clúster mediante el punto de conexión de clúster y en el modo de conjunto de réplicas (consulte Conexión a Amazon DocumentDB como conjunto de réplicas), a no ser que tenga un caso de uso específico para conectarse al punto de conexión del lector o a un punto de conexión de instancia. Para dirigir solicitudes a las réplicas, elija una configuración de preferencia de lectura de controlador que maximice el escalado de lectura mientras cumple con los requisitos de coherencia de lectura de su aplicación. Las preferencias de lectura `secondaryPreferred` permiten las lecturas de réplica y libera la instancia principal para hacer más trabajo.

Los siguientes puntos de conexión están disponibles en un clúster de Amazon DocumentDB.

Punto de conexión de clúster

El punto de conexión del clúster le conecta a la instancia principal del clúster. El punto de conexión del clúster se puede utilizar para operaciones de lectura y escritura. Un clúster de Amazon DocumentDB tiene exactamente un punto de conexión de clúster.

El punto de conexión del clúster proporciona conmutación por error para conexiones de lectura y escritura con el clúster. Si la instancia principal actual del clúster produce un error y el clúster tiene al menos una réplica de lectura activa, el punto de conexión del clúster redirige automáticamente las solicitudes de conexión a una nueva instancia principal. Cuando se conecte al clúster de Amazon DocumentDB, le recomendamos que se conecte al clúster mediante el punto de conexión de clúster y en el modo de conjunto de réplicas (consulte Conexión a Amazon DocumentDB como conjunto de réplicas).

A continuación, se muestra un punto de conexión de un clúster de Amazon DocumentDB de ejemplo:

```
sample-cluster.cluster-123456789012.us-east-1.docdb.amazonaws.com:27017
```

A continuación, se muestra una cadena de conexión de ejemplo que usa este punto de conexión de clúster:

```
mongodb://username:password@sample-cluster.cluster-123456789012.us-
east-1.docdb.amazonaws.com:27017
```

Para obtener información acerca de cómo encontrar los puntos de conexión de un clúster, consulte Búsqueda de puntos de conexión de un clúster.

Punto de conexión del lector

El punto de conexión del lector balancea la carga de las conexiones de solo lectura entre todas las réplicas disponibles del clúster. Un punto de conexión de lector de clúster funcionará como punto de conexión del clúster si se conecta a través del modo `replicaSet`, es decir, en la cadena de conexión, el parámetro del conjunto de réplicas es `&replicaSet=rs0`. En este caso, podrá llevar a cabo operaciones de escritura en el principal. Sin embargo, si se conecta al clúster que especifica `directConnection=true` y se intenta llevar a cabo una operación de escritura a través de una conexión con el punto de conexión de lector, se produce un error. Un clúster de Amazon DocumentDB tiene exactamente un punto de conexión de lector.

Si el clúster contiene solo una instancia principal, el punto de conexión del lector se conecta a la instancia principal. Cuando se añade una instancia de réplica al clúster de Amazon DocumentDB, el punto de conexión del lector abre las conexiones de solo lectura con la nueva réplica una vez que esté activo.

A continuación, se muestra un punto de conexión del lector de ejemplo de un clúster de Amazon DocumentDB:

```
sample-cluster.cluster-ro-123456789012.us-east-1.docdb.amazonaws.com:27017
```

A continuación, se muestra una cadena de conexión de ejemplo que usa un punto de conexión de lector:

```
mongodb://username:password@sample-cluster.cluster-ro-123456789012.us-
east-1.docdb.amazonaws.com:27017
```

El punto de conexión del lector balancea la carga de las conexiones de solo lectura, no de las solicitudes de lectura. Si algunas de las conexiones del punto de conexión del lector se utilizan más que otras, es posible que las solicitudes de lectura no se puedan equilibrar uniformemente entre las instancias del clúster. Se recomienda distribuir solicitudes mediante la conexión al punto de conexión de clúster como un conjunto de réplicas y mediante la opción de preferencia de lectura secondaryPreferred.

Para obtener información acerca de cómo encontrar los puntos de conexión de un clúster, consulte Búsqueda de puntos de conexión de un clúster.

Punto de conexión de instancia

Un punto de conexión de una instancia se conecta a una instancia específica del clúster. El punto de conexión de instancia de la instancia principal actual se puede utilizar para realizar operaciones de lectura y escritura. Sin embargo, si se intentan realizar operaciones de escritura en un punto de conexión de instancia de una réplica de lectura, se produce un error. Un clúster de Amazon DocumentDB tiene un punto de conexión de instancia para cada instancia activa.

Un punto de conexión de instancia proporciona un control directo sobre las conexiones con una instancia específica en los casos en los que el uso del punto de conexión del clúster o del lector puede no ser adecuado. Un ejemplo de caso de uso es el aprovisionamiento de una carga de trabajo de análisis diarios de solo lectura. Puede aprovisionar una instancia de larger-than-normal réplica, conectarse directamente a la nueva instancia más grande con su punto de enlace de instancia, ejecutar las consultas de análisis y, a continuación, cerrar la instancia. El uso del punto de conexión de instancia impide que el tráfico de los análisis afecte a otras instancias del clúster.

A continuación, se muestra un punto de conexión de instancia de ejemplo para una sola instancia de un clúster de Amazon DocumentDB:

```
sample-instance.123456789012.us-east-1.docdb.amazonaws.com:27017
```

A continuación, se muestra una cadena de conexión de ejemplo que usa este punto de conexión de instancia:

```
mongodb://username:password@sample-instance.123456789012.us-
east-1.docdb.amazonaws.com:27017
```

> **Note**
>
> El rol de instancia principal o réplica de una instancia puede cambiar debido a un evento de conmutación por error. Las aplicaciones no deben presuponer en ningún momento que un determinado punto de conexión de instancia es la instancia principal. No se recomienda conectarse a puntos de conexión de instancia para aplicaciones de producción. En su lugar, se recomienda que se conecte al clúster mediante el punto de conexión de clúster y en el modo de conjunto de réplicas (consulte Conexión a Amazon DocumentDB como conjunto de réplicas). Para obtener información sobre el control avanzado de la prioridad de conmutación por error de las instancias, consulte Información general de la tolerancia a errores de clúster de Amazon DocumentDB.

Para obtener información acerca de cómo encontrar los puntos de conexión de un clúster, consulte Búsqueda del punto de conexión de una instancia.

Modo de conjunto de réplicas

Puede conectarse al punto de conexión de su clúster de Amazon DocumentDB en modo de conjunto de réplicas especificando el nombre del conjunto de réplicas `rs0`. La conexión en el modo de conjunto de réplicas proporciona la capacidad de especificar las opciones Read Concern, Write Concern y Read Preference. Para obtener más información, consulte Coherencia de lectura.

A continuación, se muestra una cadena de conexión de ejemplo que se conecta en el modo de conjunto de réplicas:

```
mongodb://username:password@sample-cluster.cluster-123456789012.us-
east-1.docdb.amazonaws.com:27017/?replicaSet=rs0
```

Cuando se conecta en modo de conjunto de réplicas, el clúster de Amazon DocumentDB se muestra ante los controladores y clientes como un conjunto de réplicas. Las instancias añadidas y eliminadas del clúster de Amazon DocumentDB se reflejan automáticamente en la configuración del conjunto de réplicas.

Cada clúster de Amazon DocumentDB consta de un único conjunto de réplicas con el nombre predeterminado `rs0`. El nombre del conjunto de réplicas no se puede modificar.

La conexión al punto de conexión del clúster en el modo de conjunto de réplicas es el método recomendado para uso general.

> **Note**
>
> Todas las instancias de un clúster de Amazon DocumentDB atienden las conexiones en el mismo puerto TCP.

Compatibilidad con TLS

Para obtener más información sobre cómo conectarse a Amazon DocumentDB mediante seguridad de la capa de transporte (TLS), consulte Cifrado de datos en tránsito.

Almacenamiento de Amazon DocumentDB

Los datos de Amazon DocumentDB se almacenan en un volumen de clúster, que es un volumen virtual único que utiliza unidades de estado sólido ()SSDs. Un volumen de clúster se compone de seis copias de los datos, que se replican automáticamente en varias zonas de disponibilidad de una sola Región de AWS. Esta replicación ayuda a garantizar que los datos se conserven durante mucho tiempo, con menos riesgo de que se pierdan los datos. También ayuda a garantizar que el clúster esté más disponible durante una conmutación por error, porque ya existen copias de sus datos en otras zonas de disponibilidad. Estas copias pueden seguir enviando solicitudes de datos a las instancias del clúster de Amazon DocumentDB.

Cómo se factura el almacenamiento de datos de

Amazon DocumentDB aumenta automáticamente el tamaño del volumen del clúster cuando aumenta la cantidad de datos. Un volumen de clúster de Amazon DocumentDB puede crecer hasta un tamaño máximo de 128 TiB; sin embargo, solo se le cobrará por el espacio que utilice en un volumen de clúster de Amazon DocumentDB. A partir de Amazon DocumentDB 4.0, cuando se eliminan datos, por ejemplo, al eliminar una colección o un índice, el espacio asignado general disminuye en una cantidad comparable. Por lo tanto, puede reducir los cargos de almacenamiento eliminando tablas, índices y bases de datos que ya no necesite. En la versión 3.6 de Amazon DocumentDB, el volumen del clúster puede reutilizar el espacio liberado al eliminar datos, pero el volumen en sí nunca disminuye de tamaño. Como resultado, en la versión 3.6, es posible que no vea ningún cambio en el almacenamiento cuando elimine una colección o un índice, aunque el espacio liberado se vuelva a utilizar.

> **Note**
>
> Con Amazon DocumentDB 3.6, los costos de almacenamiento se basan en el “límite máximo” de almacenamiento (la cantidad máxima que se asignó al clúster de Amazon DocumentDB en cualquier momento). Puede administrar los costos evitando las prácticas de ETL que crean grandes volúmenes de información temporal o que cargan grandes volúmenes de datos nuevos antes de eliminar datos antiguos innecesarios. Si la eliminación de datos de un clúster de Amazon DocumentDB produce una cantidad sustancial de espacio asignado pero que no se utiliza, el restablecimiento del nivel máximo de crecimiento exige realizar el volcado de datos lógicos y restablecerlo a un clúster nuevo, con una herramienta como `mongodump` o `mongorestore`. La creación y restauración de una instantánea no

reduce el almacenamiento asignado debido a que la distribución física del almacenamiento subyacente no se verá modificada en la instantánea restaurada.

> **Note**
>
> El uso de `mongodump` utilidades `mongorestore` como esta I/O conlleva gastos en función del tamaño de los datos que se leen y escriben en el volumen de almacenamiento.

Para obtener información sobre el almacenamiento de datos y los precios de Amazon DocumentDB, consulte I/O precios y precios de Amazon DocumentDB (compatible con MongoDB). FAQs

Replicación de Amazon DocumentDB

En un clúster de Amazon DocumentDB, cada instancia de réplica expone un punto de conexión independiente. Los puntos de conexión de estas réplicas proporcionan acceso de solo lectura a los datos del volumen de clúster. Le permiten escalar la carga de trabajo de lectura de los datos entre varias instancias replicadas. También ayudan a mejorar el rendimiento de las lecturas de datos y a aumentar la disponibilidad de los datos en el clúster de Amazon DocumentDB. Las réplicas de Amazon DocumentDB también son objetivos de conmutación por error y se promocionan rápidamente si se produce un error en la instancia principal del clúster de Amazon DocumentDB.

Fiabilidad de Amazon DocumentDB

Amazon DocumentDB está diseñado para ofrecer fiabilidad, durabilidad y tolerancia a errores. (Para mejorar la disponibilidad, debe configurar el clúster de Amazon DocumentDB de modo que tenga varias instancias de réplica en distintas zonas de disponibilidad). Amazon DocumentDB también incluye varias características automáticas que la convierten en una solución de base de datos de confianza.

Reparación automática del almacenamiento

Amazon DocumentDB mantiene varias copias de los datos en tres zonas de disponibilidad, lo que reduce considerablemente la posibilidad de pérdida de datos debido a un error de almacenamiento. Amazon DocumentDB también detecta automáticamente los errores del volumen de clúster. Cuando se produce un error en un segmento de un volumen del clúster, Amazon DocumentDB lo repara inmediatamente. Utiliza los datos de los demás volúmenes que conforman el volumen del clúster

para ayudar a garantizar que los datos del segmento reparado estén actualizados. Como resultado, Amazon DocumentDB evita la pérdida de datos y reduce la necesidad de realizar una point-in-time restauración para recuperarse de un error de instancia.

Calentamiento de caché que puede sobrevivir

Amazon DocumentDB administra su caché de páginas en un proceso independiente de la base de datos para que pueda sobrevivir independientemente de la base de datos. En el improbable caso de que se produzca un error de la base de datos, la caché de páginas permanece en la memoria. De este modo, se garantiza que el grupo del búfer contiene datos con el estado más actualizado al reiniciar la base de datos.

Recuperación de bloqueos

Amazon DocumentDB se ha diseñado para recuperarse de un bloqueo casi instantáneamente y continuar sirviendo sus datos de aplicación sin el registro binario. Amazon DocumentDB realiza las recuperaciones de bloqueos de forma asíncrona en subprocesos paralelos, de forma que su base de datos permanece abierta y disponible inmediatamente después de un bloqueo.

Administración de recursos

Amazon DocumentDB protege los recursos necesarios para ejecutar los procesos críticos del servicio, como las comprobaciones de estado. Para ello, y cuando una instancia experimente una presión de memoria elevada, Amazon DocumentDB limitará las solicitudes. Como resultado, es posible que algunas operaciones se pongan en cola para esperar a que disminuya la presión sobre la memoria. Si la presión de la memoria continúa, es posible que se agote el tiempo de espera de las operaciones en cola. Puede controlar si el servicio limita o no sus operaciones debido a la falta de memoria con las siguientes CloudWatch métricas:`LowMemThrottleQueueDepth`,,,`LowMemThrottleMaxQueueDepth`. `LowMemNumOperationsThrottled` `LowMemNumOperationsTimedOut` Para obtener más información, consulte Supervisión de Amazon DocumentDB con. CloudWatch Si observa una presión de memoria constante en su instancia como resultado de las LowMem CloudWatch métricas, le recomendamos que amplíe la instancia para proporcionar memoria adicional para su carga de trabajo.

Opciones de preferencia de lectura

Amazon DocumentDB utiliza un servicio de almacenamiento compartido nativo en la nube que replica los datos seis veces en tres zonas de disponibilidad para ofrecer altos niveles de durabilidad.

Amazon DocumentDB no se basa en la replicación de datos en varias instancias para lograr durabilidad. Los datos del clúster serán duraderos tanto si este contiene una sola instancia como si tiene 15.

Temas

- Durabilidad de escritura
- Aislamiento de lectura
- Coherencia de lectura
- Alta disponibilidad
- Escalado de operaciones de lectura

Durabilidad de escritura

Amazon DocumentDB utiliza un sistema de almacenamiento único, distribuido, tolerante a errores y de recuperación automática. Este sistema replica seis copias (V=6) de sus datos en tres zonas de disponibilidad para ofrecer una AWS alta disponibilidad y durabilidad. Al escribir datos, Amazon DocumentDB garantiza que todas las escrituras se registren de forma duradera en la gran mayoría de los nodos antes de confirmar la escritura al cliente. Si ejecuta un conjunto de réplicas de MongoDB de tres nodos y utiliza la opción Write Concern de `{w:3, j:true}`, obtendría la mejor configuración posible en comparación con Amazon DocumentDB.

Las operaciones de escritura en el clúster de Amazon DocumentDB debe procesarlas la instancia principal del clúster. Si se intenta escribir a una réplica, se producirá un error. Una operación de escritura confirmada desde una instancia principal de Amazon DocumentDB es duradera y no se puede revertir. Amazon DocumentDB es muy duradero de forma predeterminada y no admite una opción de escritura no duradera. No se puede modificar el nivel de durabilidad (es decir, Write Concern). Amazon DocumentDB ignora w=anything y, de hecho, es w: 3 y j: true. No puede reducirlo.

Debido a que en la arquitectura de Amazon DocumentDB la computación y el almacenamiento están separados, un clúster con una sola instancia es de larga duración. La durabilidad se gestiona en la capa de almacenamiento. Como resultado, un clúster de Amazon DocumentDB con una sola instancia y uno con tres instancias consiguen el mismo nivel de durabilidad. Puede configurar el clúster para que se adapte a su caso de uso específico a la vez que proporciona un alto nivel de durabilidad para sus datos.

Las operaciones de escritura en un clúster de Amazon DocumentDB son atómicas dentro del mismo documento.

Amazon DocumentDB no admite la opción `wtimeout` y no devolverá un error si se especifica un valor. Las operaciones de escritura en la instancia principal de Amazon DocumentDB están aseguradas contra el bloqueo indefinido.

Aislamiento de lectura

Las operaciones de lectura de una instancia de Amazon DocumentDB solo devuelven datos que se conservan antes de que se inicie la consulta. Las operaciones de lectura nunca devuelven datos modificados una vez que se inicia la ejecución de la consulta, y las lecturas sucias no son posibles en ninguna circunstancia.

Coherencia de lectura

Los datos leídos de un clúster de Amazon DocumentDB son duraderos y no se pueden revertir. Puede modificar la lectura consistente para las operaciones de lectura de Amazon DocumentDB especificando la preferencia de lectura de la solicitud o conexión. Amazon DocumentDB no admite una opción de lectura no duradera.

Las lecturas de la instancia principal de un clúster de Amazon DocumentDB son muy consistentes en condiciones de funcionamiento normales y tienen read-after-write consistencia. Si se produce un evento de conmutación por error entre la escritura y la lectura posterior, el sistema puede devolver brevemente una lectura que no tiene una consistencia alta. Todas las lecturas que se realizan desde una réplica de lectura tienen consistencia final y devuelven los datos en el mismo orden, a menudo con un retardo de réplica inferior a los 100 ms.

Preferencias de lectura de Amazon DocumentDB

Amazon DocumentDB permite configurar una opción de preferencia de lectura únicamente cuando los datos se leen del punto de conexión del clúster en modo de conjunto de réplicas. La configuración de una opción de preferencia de lectura afecta al modo en que el cliente o el controlador de MongoDB lee las solicitudes enviadas a las instancias del clúster de Amazon DocumentDB. Puede definir opciones de preferencia de lectura para una consulta específica o como una opción general en el controlador de MongoDB. (Consulte la documentación del cliente o controlador para obtener instrucciones sobre cómo definir una opción de preferencia de lectura).

Si el cliente o controlador no se conecta a un punto de conexión del clúster de Amazon DocumentDB en modo de conjunto de réplicas, el resultado de especificar una preferencia de lectura es incierto.

Amazon DocumentDB no admite la configuración de conjuntos de etiquetas como preferencia de lectura.

Opciones de preferencia de lectura admitidas

- **`primary`**. especificar una preferencia de `primary` lectura ayuda a garantizar que todas las lecturas se dirijan a la instancia principal del clúster. Si la instancia principal no está disponible, se produce un error en la operación de lectura. Una preferencia de `primary` lectura proporciona read-after-write coherencia y es adecuada para los casos de uso que dan prioridad a la read-after-write coherencia por encima de la alta disponibilidad y el escalado de lectura.

  En el siguiente ejemplo se especifica una preferencia de lectura `primary`:

  ```
  db.example.find().readPref('primary')
  ```

- **`primaryPreferred`**: si se especifica una preferencia de `primaryPreferred` lectura, las lecturas se redirigen a la instancia principal en condiciones normales de funcionamiento. Si se produce una conmutación por error de la instancia principal, el cliente envía las solicitudes a una réplica. Una preferencia de `primaryPreferred` lectura proporciona read-after-write consistencia durante el funcionamiento normal y, en última instancia, lecturas consistentes durante un evento de conmutación por error. Una preferencia de `primaryPreferred` lectura es adecuada para los casos de uso que dan prioridad a la read-after-write coherencia por encima del escalado de lectura, pero que aún así requieren una alta disponibilidad.

  En el siguiente ejemplo se especifica una preferencia de lectura `primaryPreferred`:

  ```
  db.example.find().readPref('primaryPreferred')
  ```

- **`secondary`**: la especificación de una preferencia de `secondary` lectura garantiza que las lecturas solo se enruten a una réplica, nunca a la instancia principal. Si no hay instancias de réplica en el clúster, la solicitud de lectura produce un error. Al final, una preferencia de `secondary` lectura produce lecturas consistentes y es adecuada para los casos de uso en los que se da prioridad al rendimiento de escritura de la instancia principal por encima de la alta disponibilidad y read-after-write la coherencia.

  En el siguiente ejemplo se especifica una preferencia de lectura `secondary`:

  ```
  db.example.find().readPref('secondary')
  ```

- **`secondaryPreferred`**: la especificación de una preferencia de `secondaryPreferred` lectura garantiza que las lecturas se enruten a una réplica de lectura cuando hay una o más réplicas activas. Si no hay instancias de réplica activas en el clúster, la solicitud de lectura se envía a la instancia principal. Una preferencia de lectura `secondaryPreferred` proporciona operaciones de lectura consistente final cuando una réplica de lectura atiende la operación de lectura. Proporciona read-after-write coherencia cuando la lectura la realiza la instancia principal (salvo que se produzcan eventos de conmutación por error). La preferencia de `secondaryPreferred` lectura es adecuada para los casos de uso que dan prioridad a la escalabilidad de la lectura y a la alta disponibilidad por encima de la coherencia. read-after-write

  En el siguiente ejemplo se especifica una preferencia de lectura `secondaryPreferred`:

  ```
  db.example.find().readPref('secondaryPreferred')
  ```

- **`nearest`**: al especificar una preferencia de `nearest` lectura, las lecturas se distribuyen únicamente en función de la latencia medida entre el cliente y todas las instancias del clúster de Amazon DocumentDB. Una preferencia de lectura `nearest` proporciona operaciones de lectura consistente final cuando una réplica de lectura atiende la operación de lectura. Ofrece read-after-write coherencia cuando la lectura la realiza la instancia principal (salvo los eventos de conmutación por error). La preferencia de `nearest` lectura es adecuada para los casos de uso en los que se da prioridad a lograr la latencia de lectura y la alta disponibilidad más bajas posibles por encima de la read-after-write coherencia y el escalado de lectura.

  En el siguiente ejemplo se especifica una preferencia de lectura `nearest`:

  ```
  db.example.find().readPref('nearest')
  ```

Alta disponibilidad

Amazon DocumentDB admite configuraciones de clúster altamente disponibles mediante el uso de réplicas como destinos de la conmutación por error de la instancia principal. Si la instancia principal produce un error, una réplica de Amazon DocumentDB pasará a ser la nueva instancia principal, con una breve interrupción durante la cual las solicitudes de lectura y escritura realizadas a la instancia principal producen una excepción.

Si el clúster de Amazon DocumentDB no contiene réplicas, se vuelve a crear la instancia principal cuando se produce un error. Sin embargo, promover una réplica de Amazon DocumentDB es mucho más rápido que volver a crear la instancia principal. Por lo tanto, le recomendamos que cree una o varias réplicas de Amazon DocumentDB como destinos de conmutación por error.

Las réplicas que se han diseñado para utilizarlas como destinos de conmutación por error deben ser de la misma clase de instancia que la instancia principal. Deberían aprovisionarse en zonas de disponibilidad distintas de la principal. Puede controlar las réplicas que deben usarse como destinos de la conmutación por error. Para obtener instrucciones sobre cómo configurar Amazon DocumentDB para una alta disponibilidad, consulte Información general de la tolerancia a errores de clúster de Amazon DocumentDB.

Escalado de operaciones de lectura

Las réplicas de Amazon DocumentDB son ideales para el escalado de lectura. Están totalmente dedicadas a las operaciones de lectura en el volumen del clúster, es decir, las réplicas no procesan operaciones de escritura. La replicación de datos se produce en el volumen del clúster y no entre las instancias. Por lo tanto, los recursos de cada réplica se dedican a procesar las consultas, y no a replicar y escribir datos.

Si su aplicación necesita más capacidad de lectura, puede añadir una réplica al clúster rápidamente (normalmente en menos de 10 minutos). Si los requisitos de capacidad de lectura disminuyen, puede eliminar las réplicas que no necesite. Con las réplicas de Amazon DocumentDB, solo paga por la capacidad de lectura que necesite.

Amazon DocumentDB permite el escalado de lectura en el cliente mediante el uso de opciones de preferencia de lectura. Para obtener más información, consulte Preferencias de lectura de Amazon DocumentDB.

Eliminaciones de TTL

Las eliminaciones de un área de índice TTL logradas a través de un proceso en segundo plano son el mejor esfuerzo y no están garantizadas dentro de un período de tiempo específico. Factores como el tamaño de instancia, la utilización de recursos de instancia, el tamaño del documento y el rendimiento general pueden afectar la temporización de una eliminación de TTL.

Cuando el monitor TTL elimina sus documentos, cada eliminación incurre en costos de E/S, lo que aumentará su factura. Si el rendimiento y las tasas de eliminación de TTL aumentan, debería esperar un aumento en su factura debido al aumento del uso de E/S.

Al crear un índice TTL en una colección existente, debe eliminar todos los documentos caducados antes de crear el índice. La implementación actual del TTL está optimizada para eliminar una pequeña fracción de los documentos de la colección, lo que suele ocurrir si el TTL estaba activado en la colección desde el principio, y puede resultar en un aumento de las IOPS de lo necesario si es necesario eliminar un gran número de documentos de una sola vez.

En lugar de utilizar un índice TTL para eliminar documentos, puede segmentar documentos en colecciones según el tiempo y simplemente eliminar esas colecciones cuando los documentos ya no sean necesarios. Por ejemplo: puede crear una colección por semana y eliminarla sin incurrir en costos de E/S. Esto puede resultar considerablemente más rentable que utilizar un índice TTL.

Recursos facturables

Identificación de los recursos facturables de Amazon DocumentDB

Como base de datos administrada, Amazon DocumentDB cobra por las instancias, el almacenamiento, las E/S, las copias de seguridad y la transferencia de datos. Para obtener más información, consulte Amazon DocumentDB (with MongoDB compatibility) Pricing.

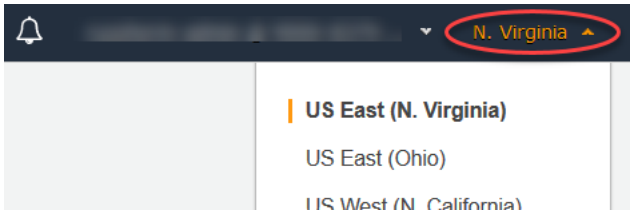
Para descubrir los recursos facturables de tu cuenta y, si es posible, eliminarlos, puedes usar la opción Consola de administración de AWS o AWS CLI.

Usando el Consola de administración de AWS

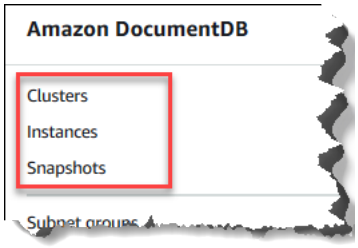
Con el Consola de administración de AWS, puede descubrir los clústeres, instancias e instantáneas de Amazon DocumentDB que ha aprovisionado para un determinado número. Región de AWS

Para detectar clústeres, instancias e instantáneas

1. Inicie sesión en y abra la Consola de administración de AWS consola de Amazon DocumentDB en https://console.aws.amazon.com /docdb.
2. Para descubrir los recursos facturables en una región que no sea la región predeterminada, en la esquina superior derecha de la pantalla, elija la Región de AWS que desee buscar.



3. En el panel de navegación, seleccione el tipo de recurso facturable que le interesa: Clusters (Clústeres), Instances (Instancias) o Snapshots (Instantáneas).



4. Todos los clústeres, instancias o instantáneas aprovisionados para la región se indican en el panel de la derecha. Se le cobrará por los clústeres, las instancias y las instantáneas.

Usando el AWS CLI

Con el AWS CLI, puede descubrir los clústeres, instancias e instantáneas de Amazon DocumentDB que ha aprovisionado para un determinado número. Región de AWS

Para detectar clústeres e instancias

El código siguiente muestra todos los clústeres e instancias para la región especificada. Si desea buscar clústeres e instancias en la región predeterminada, puede omitir el parámetro `--region`.

Example

Para Linux, macOS o Unix:

```
aws docdb describe-db-clusters \
    --region us-east-1 \
    --query 'DBClusters[?Engine==`docdb`]' | \
       grep -e "DBClusterIdentifier" -e "DBInstanceIdentifier"
```

Para Windows:

```
aws docdb describe-db-clusters ^
    --region us-east-1 ^
    --query 'DBClusters[?Engine==`docdb`]' | ^
       grep -e "DBClusterIdentifier" -e "DBInstanceIdentifier"
```

La salida de esta operación será similar a lo que se indica a continuación.

```
"DBClusterIdentifier": "docdb-2019-01-09-23-55-38",
        "DBInstanceIdentifier": "docdb-2019-01-09-23-55-38",
        "DBInstanceIdentifier": "docdb-2019-01-09-23-55-382",
```

```
"DBClusterIdentifier": "sample-cluster",
"DBClusterIdentifier": "sample-cluster2",
```

Para detectar instantáneas

El código siguiente muestra todas las instantáneas para la región especificada. Si desea buscar instantáneas en la región predeterminada, puede omitir el parámetro `--region`.

Para Linux, macOS o Unix:

```
aws docdb describe-db-cluster-snapshots \
  --region us-east-1 \
  --query 'DBClusterSnapshots[?Engine==`docdb`].
[DBClusterSnapshotIdentifier,SnapshotType]'
```

Para Windows:

```
aws docdb describe-db-cluster-snapshots ^
  --region us-east-1 ^
  --query 'DBClusterSnapshots[?Engine==`docdb`].
[DBClusterSnapshotIdentifier,SnapshotType]'
```

La salida de esta operación será similar a lo que se indica a continuación.

```
[
    [
        "rds:docdb-2019-01-09-23-55-38-2019-02-13-00-06",
        "automated"
    ],
    [
        "test-snap",
        "manual"
    ]
]
```

Solo tiene que eliminar las instantáneas `manual`. Las instantáneas `Automated` se eliminan cuando elimina el clúster.

Eliminación de recursos facturables no deseados

Para eliminar un clúster, antes debe eliminar todas las instancias de ese clúster.

- Para eliminar las instancias, consulte Eliminación de una instancia de Amazon DocumentDB.

> **Important**
>
> Aunque elimine las instancias de un clúster, se le seguirá facturando por el uso del almacenamiento y las copias de seguridad asociadas a ese clúster. Para evitar todos los cargos, también debe eliminar el clúster y las instantáneas manuales.

- Para eliminar clústeres, consulte Eliminación de un clúster de Amazon DocumentDB.
- Para eliminar instantáneas manuales, consulte Eliminación de una instantánea del clúster.

¿Qué es una base de datos de documentos?

Algunos desarrolladores no piensan en su modelo de datos en términos de filas y columnas normalizadas. Normalmente, en la capa de aplicación, los datos se representan como un documento JSON, porque es más intuitivo para los desarrolladores pensar en su modelo de datos como un documento.

La popularidad de las bases de datos documentales ha aumentado porque permiten conservar los datos en una base de datos utilizando el mismo formato de modelo de documentos que se usa en el código de la aplicación. Las bases de datos documentales proporcionan API eficaces e intuitivas que permiten un desarrollo flexible y ágil.

Temas

- Casos de uso de bases de datos de documentos
- Descripción de documentos
- Trabajo con documentos

Casos de uso de bases de datos de documentos

La necesidad de usar una base de datos documental u otro tipo de base de datos para administrar los datos dependerá del caso de uso. Las bases de datos documentales son útiles para cargas de trabajo que requieren un esquema flexible que permita un desarrollo rápido e iterativo. A continuación, se incluyen algunos ejemplos de casos de uso para los que las bases de datos documentales pueden ofrecer importantes ventajas:

Temas

- Perfiles de usuario
- Big data en tiempo real
- Administración de contenido

Perfiles de usuario

Como las bases de datos documentales tienen un esquema flexible, pueden almacenar documentos que tengan atributos y valores de datos diferentes. Las bases de datos documentales son una solución práctica para los perfiles online en los que diferentes usuarios proporcionan diferentes tipos de información. Mediante una base de datos documental, puede almacenar cada perfil de usuario de forma eficaz almacenando solo los atributos que son específicos de cada usuario.

Suponga que un usuario decide añadir o eliminar la información de su perfil. En este caso, su documento podría reemplazarse fácilmente por una versión actualizada que contuviera los atributos y datos recién añadidos u omitir todos los atributos y datos recién omitidos. Las bases de datos documentales administran fácilmente este nivel de detalle y fluidez.

Big data en tiempo real

Históricamente, la capacidad de extraer información de datos operativos se ha visto obstaculizada por el hecho de que las bases de datos operativas y las bases de datos de análisis se mantenían en diferentes entornos informes operativos y de negocio, respectivamente. Ser capaces de extraer información operativa en tiempo real es fundamental en un entorno empresarial altamente competitivo. Mediante el uso de bases de datos documentales, una empresa puede almacenar y administrar datos operativos de cualquier origen e incluir los datos de forma simultánea en el motor de BI elegido para su análisis. No es necesario tener dos entornos.

Administración de contenido

Para administrar eficazmente el contenido, debe poder recopilar y agrupar contenido de una variedad de orígenes y enviárselo al cliente. Debido a su esquema flexible, las bases de datos documentales son perfectas para recopilar y almacenar cualquier tipo de datos. Puede utilizarlas para crear e incorporar nuevos tipos de contenido, incluido el contenido generado por el usuario, como imágenes, comentarios, y vídeos.

Descripción de documentos

Las bases de datos de documentos se utilizan para almacenar datos semiestructurados como un documento en lugar de normalizar los datos entre varias tablas, cada una con una estructura única

y fija, como en una base de datos relacional. Los documentos almacenados en una base de datos documental usan pares de clave-valor anidados para proporcionar la estructura o el esquema del documento. Sin embargo, se pueden almacenar diferentes tipos de documentos en la misma base de datos documental, cumpliendo así el requisito de procesar datos similares que tienen diferentes formatos. Por ejemplo, como cada documento es autodescriptivo, los documentos codificados en JSON para una tienda online que se describen en el tema Documentos de ejemplo en una base de datos de documentos se pueden almacenar en la misma base de datos documental.

Temas

- Terminología SQL frente a terminología no relacional
- Documentos simples
- Documentos incrustados
- Documentos de ejemplo en una base de datos de documentos
- Descripción de la normalización en una base de datos de documentos

Terminología SQL frente a terminología no relacional

En la tabla siguiente se compara la terminología utilizada en las bases de datos documentales (MongoDB) con la terminología utilizada en las bases de datos SQL.

SQL	MongoDB
Tabla	Recopilación
Fila	Documento
Columna	Campo
Clave principal	ObjectId
Index	Index
Visualización	Visualización
Tabla u objeto anidado	Documento incrustado
Matriz	Matriz

Documentos simples

Todos los documentos de una base de datos documental son autodescriptivos. En esta documentación, se utilizan documentos con formato JSON, pero se podrían usar otros medios de codificación.

Un documento simple tiene uno o varios campos que están en el mismo nivel del documento. En el siguiente ejemplo, los campos `SSN`, `LName`, `FName`, `DOB`, `Street`, `City`, `State-Province`, `PostalCode` y `Country` son todos elementos del mismo nivel en el documento.

```
{
   "SSN": "123-45-6789",
   "LName": "Rivera",
   "FName": "Martha",
   "DOB": "1992-11-16",
   "Street": "125 Main St.",
   "City": "Anytown",
   "State-Province": "WA",
   "PostalCode": "98117",
   "Country": "USA"
}
```

Cuando la información está organizada en un documento simple, cada campo se administra por separado. Para recuperar la dirección de una persona, debe recuperar `Street`, `City`, `State-Province`, `PostalCode` y `Country` como elementos de datos individuales.

Documentos incrustados

Un documento complejo organiza sus datos mediante la creación de documentos incrustados en el documento. Los documentos incrustados ayudan a administrar los datos en grupos y como elementos de datos individuales, lo que sea más eficaz para cada caso. Utilizando el ejemplo anterior, podría incrustar un documento `Address` en el documento principal, lo que produciría la siguiente estructura de documentos:

```
{
   "SSN": "123-45-6789",
   "LName": "Rivera",
   "FName": "Martha",
   "DOB": "1992-11-16",
   "Address":
   {
```

```
        "Street": "125 Main St.",
        "City": "Anytown",
        "State-Province": "WA",
        "PostalCode": "98117",
        "Country": "USA"
    }
}
```

Ahora puede obtener acceso a los datos del documento como campos individuales (`"SSN":`), como un documento incrustado (`"Address":`) o como un miembro de un documento incrustado (`"Address":{"Street":}`).

Documentos de ejemplo en una base de datos de documentos

Como se indicó anteriormente, puesto que cada documento de una base de datos documental es autodescriptivo, la estructura de los documentos de una base de datos documental puede ser diferente. Los siguientes dos documentos, uno para un libro y otro para una publicación periódica, son diferentes estructuralmente. Sin embargo, ambos pueden estar en la misma base de datos documental.

A continuación, se muestra un documento de libro de ejemplo:

```
{
    "_id" : "9876543210123",
    "Type": "book",
    "ISBN": "987-6-543-21012-3",
    "Author":
    {
        "LName":"Roe",
        "MI": "T",
        "FName": "Richard"
    },
    "Title": "Understanding Document Databases"
}
```

A continuación, se muestra un documento de publicación periódica de ejemplo con dos artículos:

```
{
    "_id" : "0123456789012",
    "Publication": "Programming Today",
    "Issue":
```

```
    {
        "Volume": "14",
        "Number": "09"
    },
    "Articles" : [
        {
            "Title": "Is a Document Database Your Best Solution?",
            "Author":
            {
                "LName": "Major",
                "FName": "Mary"
            }
        },
        {
            "Title": "Databases for Online Solutions",
            "Author":
            {
                "LName": "Stiles",
                "FName": "John"
            }
        }
    ],
    "Type": "periodical"
}
```

Compare la estructura de estos dos documentos. Con una base de datos relacional, necesita separar las tablas "periodical" y "books", o una sola tabla con los campos no utilizados, como "Publication," "Issue," "Articles" y "MI", como valores `null`. Como las bases de datos documentales son semiestructuradas, en las que cada documento define su propia estructura, estos dos documentos pueden coexistir en la misma base de datos documental sin campos `null`. Las bases de datos documentales son adecuadas para trabajar con datos dispersos.

El desarrollo de una base de datos documental permite el desarrollo rápido e iterativo. Esto se debe a que puede cambiar la estructura de los datos de un documento de forma dinámica, sin tener que cambiar el esquema de toda la colección. Las bases de datos documentales están especialmente indicadas para un desarrollo ágil y para entornos que cambian dinámicamente.

Descripción de la normalización en una base de datos de documentos

Las bases de datos documentales no están normalizadas; los datos que se encuentran en un documento se pueden repetir en otro documento. Asimismo, puede haber discrepancias de datos entre los documentos. Considere, por ejemplo, un escenario en el que realiza una compra en

una tienda online y todos los detalles de sus compras se almacenan en un único documento. El documento podría tener un aspecto similar al siguiente documento JSON:

```
{
    "DateTime": "2018-08-15T12:13:10Z",
    "LName" : "Santos",
    "FName" : "Paul",
    "Cart" : [
        {
            "ItemId" : "9876543210123",
            "Description" : "Understanding Document Databases",
            "Price" : "29.95"
        },
        {
            "ItemId" : "0123456789012",
            "Description" : "Programming Today",
            "Issue": {
                "Volume": "14",
                "Number": "09"
            },
            "Price" : "8.95"
        },
        {
            "ItemId": "234567890-K",
            "Description": "Gel Pen (black)",
            "Price": "2.49"
        }
    ],
    "PaymentMethod" :
    {
        "Issuer" : "MasterCard",
        "Number" : "1234-5678-9012-3456"
    },
    "ShopperId" : "1234567890"
}
```

Toda esta información se almacena como un documento en una colección de transacciones. Posteriormente, se da cuenta de que ha olvidado comprar un artículo. Así que vuelve a iniciar sesión en la misma tienda y realiza otra compra, que también se almacena como otro documento en la colección de transacciones.

```
{
```

```
    "DateTime": "2018-08-15T14:49:00Z",
    "LName" : "Santos",
    "FName" : "Paul",
    "Cart" : [
        {
            "ItemId" : "2109876543210",
            "Description" : "Document Databases for Fun and Profit",
            "Price" : "45.95"
        }
    ],
    "PaymentMethod" :
    {
        "Issuer" : "Visa",
        "Number" : "0987-6543-2109-8765"
    },
    "ShopperId" : "1234567890"
}
```

Observe la redundancia entre estos dos documentos: su nombre y el ID de comprador (y, si utilizó la misma tarjeta de crédito, la información de la tarjeta de crédito). Pero eso no es un problema, porque el almacenamiento es barato y cada documento registra completamente una transacción que se puede recuperar rápidamente con una sencilla consulta de clave-valor que no requiere uniones.

También hay una discrepancia aparente entre los dos documentos: la información de su tarjeta de crédito. Esta solo es una discrepancia aparente, ya que es probable que utilizara una tarjeta de crédito diferente para cada compra. Cada documento es correcto para la transacción que documenta.

Trabajo con documentos

Como base de datos de documentos, Amazon DocumentDB facilita el almacenamiento, la consulta y la indexación de datos JSON. En Amazon DocumentDB, una colección es similar a una tabla de una base de datos relacional, con la salvedad de que no se aplica ningún esquema a todos los documentos. Las colecciones le permiten agrupar documentos similares manteniéndolos en la misma base de datos, sin necesidad de que tengan la misma estructura.

Sigamos con los documentos de ejemplo de las secciones anteriores y suponga ahora que tiene colecciones para `reading_material` y `office_supplies`. Es responsabilidad de su software decidir a qué colección pertenece un documento.

En los siguientes ejemplos se utiliza la API de MongoDB para mostrar cómo añadir, consultar, actualizar y eliminar documentos.

Temas

- Adición de documentos
- Consulta de documentos
- Actualización de documentos
- Eliminación de documentos

Adición de documentos

En Amazon DocumentDB, se crea una base de datos cuando se agrega por primera vez un documento a una colección. En este ejemplo, está creando una colección denominada `example` en la base de datos `test`, que es la base de datos predeterminada cuando se conecta a un clúster. Dado que la conexión se crea implícitamente cuando se inserta el primer documento, no hay comprobación de errores del nombre de la colección. Por lo tanto, un error tipográfico en el nombre de la colección, como `eexample` en lugar de `example`, creará y agregará el documento a la colección `eexample` en lugar de la colección prevista. La comprobación de errores debe realizarla su aplicación.

En los ejemplos siguientes, se utiliza la API de MongoDB para añadir documentos.

Temas

- Adición de un solo documento
- Adición de varios documentos

Adición de un solo documento

Para añadir un único documento a una colección, utilice la operación `insertOne( {} )` con el documento que desea añadir a la colección.

```
db.example.insertOne(
    {
        "Item": "Ruler",
        "Colors": ["Red","Green","Blue","Clear","Yellow"],
        "Inventory": {
            "OnHand": 47,
```

```
            "MinOnHand": 40
        },
        "UnitPrice": 0.89
    }
)
```

La salida de esta operación será similar a lo que se indica a continuación (formato JSON).

```
{
    "acknowledged" : true,
    "insertedId" : ObjectId("5bedafbcf65ff161707de24f")
}
```

Adición de varios documentos

Para añadir varios documentos a una colección, utilice la operación `insertMany( [{},..., {}] )` con una lista de los documentos que desea añadir a la colección. Aunque los documentos de esta lista en particular tengan diferentes esquemas, se pueden añadir a la misma colección.

```
db.example.insertMany(
    [
        {
            "Item": "Pen",
            "Colors": ["Red","Green","Blue","Black"],
            "Inventory": {
                "OnHand": 244,
                "MinOnHand": 72
            }
        },
        {
            "Item": "Poster Paint",
            "Colors": ["Red","Green","Blue","Black","White"],
            "Inventory": {
                "OnHand": 47,
                "MinOnHand": 50
            }
        },
        {
            "Item": "Spray Paint",
            "Colors": ["Black","Red","Green","Blue"],
            "Inventory": {
                "OnHand": 47,
```

```
                "MinOnHand": 50,
                "OrderQnty": 36
            }
        }
    ]
)
```

La salida de esta operación será similar a lo que se indica a continuación (formato JSON).

```
{
    "acknowledged" : true,
    "insertedIds" : [
            ObjectId("5bedb07941ca8d9198f5934c"),
            ObjectId("5bedb07941ca8d9198f5934d"),
            ObjectId("5bedb07941ca8d9198f5934e")
    ]
}
```

Consulta de documentos

A veces, es posible que tenga que examinar el inventario de su tienda online para que los clientes puedan ver y comprar lo que usted vende. Consultar una colección es relativamente fácil, tanto si desea consultar todos los documentos de la colección como solo aquellos que cumplan un determinado criterio.

Para consultar documentos, utilice la operación `find()`. El comando `find()` tiene un único parámetro de documento que define los criterios que se utilizan al elegir los documentos que se devuelven. El resultado de `find()` es un documento formateado como una sola línea de texto sin saltos de línea. Para formatear el documento resultante para facilitar su lectura, utilice `find().pretty()`. En todos los ejemplos que se muestran en este tema, se utiliza `.pretty()` para formatear la salida.

Utilice los cuatro documentos que insertó en la colección `example` de los dos ejercicios anteriores `insertOne()` e `insertMany()`.

Temas

- Recuperar todos los documentos de una colección
- Recuperación de documentos que coincidan con un valor de campo
- Recuperación de documentos que coincidan con un documento incrustado

- Recuperación de documentos que coincidan con un valor de campo de un documento incrustado
- Recuperación de documentos que coincidan con una matriz
- Recuperación de documentos que coincidan con un valor de una matriz
- Recuperación de documentos mediante operadores

Recuperar todos los documentos de una colección

Para recuperar todos los documentos de la colección, utilice la operación `find()` con un documento de consulta vacío.

La siguiente consulta devuelve todos los documentos de la colección `example`.

```
db.example.find( {} ).pretty()
```

Recuperación de documentos que coincidan con un valor de campo

Para recuperar todos los documentos que coincidan con un campo y valor, utilice la operación `find()` con un documento de consulta que identifique los campos y valores que desee.

Si se utilizan los documentos anteriores, esta consulta devuelve todos los documentos cuyo campo "Item" contiene "Pen".

```
db.example.find( { "Item": "Pen" } ).pretty()
```

Recuperación de documentos que coincidan con un documento incrustado

Para buscar todos los documentos que coinciden con un documento incrustado, utilice la operación `find()` con un documento de consulta que especifique el nombre del documento incrustado y todos los campos y los valores de ese documento incrustado.

Cuando se buscan coincidencias con un documento incrustado, el documento incrustado del documento debe tener el mismo nombre que en la consulta. Además, los campos y los valores del documento incrustado deben coincidir con la consulta.

La siguiente consulta devuelve únicamente el documento "Poster Paint". Esto se debe a que "Pen" tiene diferentes valores para "`OnHand`" y "`MinOnHand`", y "Spray Paint" tiene un campo más (`OrderQnty`) que el documento de consulta.

```
db.example.find({"Inventory": {
```

```
    "OnHand": 47,
    "MinOnHand": 50 } } ).pretty()
```

Recuperación de documentos que coincidan con un valor de campo de un documento incrustado

Para buscar todos los documentos que coinciden con un documento incrustado, utilice la operación `find()` con un documento de consulta que especifique el nombre del documento incrustado y todos los campos y los valores de ese documento incrustado.

Dados los documentos anteriores, la siguiente consulta utiliza la "notación de puntos" para especificar el documento incrustado y los campos de interés. Se devolverá cualquier documento que coincida con ellos, independientemente de los otros campos que puedan existir en el documento incrustado. La consulta devuelve "Poster Paint" y "Spray Paint", ya que ambos coinciden con los campos y los valores especificados.

```
db.example.find({"Inventory.OnHand": 47, "Inventory.MinOnHand": 50 }).pretty()
```

Recuperación de documentos que coincidan con una matriz

Para buscar todos los documentos que coincidan con una matriz, utilice la operación `find()` con el nombre de la matriz que le interese y todos los valores de esa matriz. La consulta devuelve todos los documentos que tengan una matriz con ese nombre y cuyos valores de la matriz sean idénticos y estén en el mismo orden que en la consulta.

La siguiente consulta devuelve únicamente "Pen", ya que "Poster Paint" tiene un color adicional (White) y "Spray Paint" tiene los colores en otro orden.

```
db.example.find( { "Colors": ["Red","Green","Blue","Black"] } ).pretty()
```

Recuperación de documentos que coincidan con un valor de una matriz

Para buscar todos los documentos que tengan un valor determinado en una matriz, utilice la operación `find()` con el nombre de la matriz y el valor que le interese.

```
db.example.find( { "Colors": "Red" } ).pretty()
```

La operación anterior devuelve los tres documentos, ya que cada uno de ellos tiene una matriz denominada `Colors` y el valor "`Red`" en algún lugar de la matriz. Si especifica el valor "`White`", la consulta solo devolvería "Poster Paint".

Recuperación de documentos mediante operadores

La siguiente consulta devuelve todos los documentos en los que el valor de "`Inventory.OnHand`" es menor que 50.

```
db.example.find(
        { "Inventory.OnHand": { $lt: 50 } } )
```

Para obtener una lista de los operadores de consulta admitidos, consulte Operadores de consulta y proyección.

Actualización de documentos

Normalmente, los documentos no son estáticos y se actualizan como parte de los flujos de trabajo de la aplicación. En los siguientes ejemplos se muestran algunas de las formas en que puede actualizar los documentos.

Para actualizar un documento existente, use la operación `update()`. La operación `update()` tiene dos parámetros de documento. El primer documento identifica el documento o los documentos que se van a actualizar. El segundo documento especifica las actualizaciones que se deben realizar.

Al actualizar un campo existente ya sea un campo sencillo, una matriz o un documento incrustado debe especificar el nombre del campo y sus valores. Al final de la operación, es como si el campo del documento antiguo se ha sustituido por el campo y los valores nuevos.

Temas

- Actualizar los valores de un campo existente
- Agregado de un campo nuevo
- Sustitución de un documento incrustado
- Inserción de campos nuevos en un documento incrustado
- Eliminación de un campo de un documento
- Eliminación de un campo de varios documentos

Actualizar los valores de un campo existente

Utilice los cuatro documentos siguientes que ha añadido anteriormente para las siguientes operaciones de actualización.

```
{
    "Item": "Ruler",
    "Colors": ["Red","Green","Blue","Clear","Yellow"],
    "Inventory": {
        "OnHand": 47,
        "MinOnHand": 40
    },
    "UnitPrice": 0.89
},
{
    "Item": "Pen",
    "Colors": ["Red","Green","Blue","Black"],
    "Inventory": {
        "OnHand": 244,
        "MinOnHand": 72
    }
},
{
    "Item": "Poster Paint",
    "Colors": ["Red","Green","Blue","Black","White"],
    "Inventory": {
        "OnHand": 47,
        "MinOnHand": 50
    }
},
{
    "Item": "Spray Paint",
    "Colors": ["Black","Red","Green","Blue"],
    "Inventory": {
        "OnHand": 47,
        "MinOnHand": 50,
        "OrderQnty": 36
    }
}
```

Para actualizar un campo sencillo

Para actualizar un campo sencillo, utilice `update()` con `$set` para especificar el nombre del campo y el valor nuevo. En el siguiente ejemplo, se cambia `Item` de "Pen" a "Gel Pen".

```
db.example.update(
    { "Item" : "Pen" },
    { $set: { "Item": "Gel Pen" } }
```

```
)
```

Los resultados de esta operación serán similares a lo que se indica a continuación (formato JSON).

```
{
    "Item": "Gel Pen",
    "Colors": ["Red","Green","Blue","Black"],
    "Inventory": {
        "OnHand": 244,
        "MinOnHand": 72
    }
}
```

Para actualizar una matriz

En el siguiente ejemplo, se sustituye la gama de colores existente por una matriz nueva que incluye `Orange` y elimina `White` de la lista de colores. La lista de colores nueva se encuentra en el orden especificado en la operación `update()`.

```
db.example.update(
    { "Item" : "Poster Paint" },
    { $set: { "Colors": ["Red","Green","Blue","Orange","Black"] } }
)
```

Los resultados de esta operación serán similares a lo que se indica a continuación (formato JSON).

```
{
    "Item": "Poster Paint",
    "Colors": ["Red","Green","Blue","Orange","Black"],
    "Inventory": {
        "OnHand": 47,
        "MinOnHand": 50
    }
}
```

Agregado de un campo nuevo

Para modificar un documento añadiendo uno o varios campos nuevos, utilice la operación `update()` con un documento de consulta que identifique el documento que se va a insertar y los nuevos campos y valores que se van a insertar mediante el operador `$set`.

En el siguiente ejemplo, se añade el campo `UnitPrice` con el valor `3.99` en el documento Spray Paints. Tenga en cuenta que el valor `3.99` es numérico y no una cadena.

```
db.example.update(
    { "Item": "Spray Paint" },
    { $set: { "UnitPrice": 3.99 } }
)
```

Los resultados de esta operación serán similares a lo que se indica a continuación (JSON format).

```
{
    "Item": "Spray Paint",
    "Colors": ["Black","Red","Green","Blue"],
    "Inventory": {
        "OnHand": 47,
        "MinOnHand": 50,
        "OrderQnty": 36
    },
    "UnitPrice": 3.99
}
```

Sustitución de un documento incrustado

Para modificar un documento sustituyendo un documento incrustado, utilice la operación `update()` con documentos que identifiquen el documento incrustado y sus campos y valores nuevos mediante el operador `$set`.

Dado el documento siguiente.

```
db.example.insert({
    "DocName": "Document 1",
    "Date": {
        "Year": 1987,
        "Month": 4,
        "Day": 18
    }
})
```

Para sustituir un documento incrustado

En el ejemplo siguiente, se sustituye el documento Date actual por uno nuevo que solo tiene los campos `Month` y `Day` en el que se ha eliminado `Year`.

```
db.example.update(
    { "DocName" : "Document 1" },
    { $set: { "Date": { "Month": 4, "Day": 18 } } }
)
```

Los resultados de esta operación serán similares a lo que se indica a continuación (formato JSON).

```
{
    "DocName": "Document 1",
    "Date": {
        "Month": 4,
        "Day": 18
    }
}
```

Inserción de campos nuevos en un documento incrustado

Para añadir campos a un documento incrustado

Para modificar un documento añadiendo uno o varios campos nuevos a un documento incrustado, utilice la operación `update()` con documentos que identifiquen el documento incrustado y la "notación de puntos" para especificar el documento incrustado y los campos y valores nuevos que se van a insertar mediante el operador `$set`.

Teniendo en cuenta el siguiente documento, el código siguiente utiliza la "notación de puntos" para insertar los campos `Year` y `DoW` en el documento incrustado `Date` y `Words` en el documento principal.

```
{
    "DocName": "Document 1",
    "Date": {
        "Month": 4,
        "Day": 18
    }
}
```

```
db.example.update(
    { "DocName" : "Document 1" },
    { $set: { "Date.Year": 1987,
              "Date.DoW": "Saturday",
```

```
                "Words": 2482 } }
)
```

Los resultados de esta operación serán similares a lo que se indica a continuación (formato JSON).

```
{
    "DocName": "Document 1",
    "Date": {
        "Month": 4,
        "Day": 18,
        "Year": 1987,
        "DoW": "Saturday"
    },
    "Words": 2482
}
```

Eliminación de un campo de un documento

Para modificar un documento eliminando uno se sus campos, utilice la operación `update()` con un documento de consulta que identifique el documento cuyo campo se va a eliminar y el operador `$unset` para especificar campo que se va a eliminar.

En el siguiente ejemplo, se elimina el campo `Words` del documento anterior.

```
db.example.update(
    { "DocName" : "Document 1" },
    { $unset: { Words:1 } }
)
```

Los resultados de esta operación serán similares a lo que se indica a continuación (formato JSON).

```
{
    "DocName": "Document 1",
    "Date": {
        "Month": 4,
        "Day": 18,
        "Year": 1987,
        "DoW": "Saturday"
    }
}
```

Eliminación de un campo de varios documentos

Para modificar un documento mediante la eliminación de un campo de varios documentos, utilice la operación `update()` con el operador `$unset` y la opción `multi` establecida en `true`.

En el ejemplo siguiente se quita el campo `Inventory` de todos los documentos de la colección de ejemplo. Si un documento no tiene el campo `Inventory`, no se realiza ninguna acción en ese documento. Si `multi: true` se omite, la acción solo se realiza en el primer documento que cumple el criterio.

```
db.example.update(
    {},
    { $unset: { Inventory:1 } },
    { multi: true }
)
```

Eliminación de documentos

Para eliminar un documento de la base de datos, utilice la operación `remove()`, especificando el documento que se va a eliminar. El código siguiente elimina "Gel Pen" de la colección `example`.

```
db.example.remove( { "Item": "Gel Pen" } )
```

Para eliminar todos los documentos de la base de datos, use la operación `remove()` con una consulta vacía.

```
db.example.remove( { } )
```

Introducción a Amazon DocumentDB

Existen muchas formas de conectarse a Amazon DocumentDB y empezar a usarlo. Creamos esta guía porque nos pareció que era la forma más rápida, sencilla y fácil de que los usuarios comenzaran a utilizar nuestra potente base de datos de documentos. En esta guía se utiliza el AWS CloudShell para conectarse al clúster de Amazon DocumentDB directamente desde la Consola de administración de AWS y consultarlo. Los nuevos clientes que reúnan los requisitos para el nivel gratuito de AWS pueden utilizar Amazon DocumentDB y CloudShell gratis. Si su entorno AWS CloudShell o clúster de Amazon DocumentDB hace uso de recursos más allá de la capa gratuita, se le cobrarán las tarifas de AWS normales de dichos recursos. Esta guía le permitirá empezar a utilizar Amazon DocumentDB en menos de cinco minutos.

> **Note**
>
> Las instrucciones de esta guía son específicas para crear clústeres basados en instancias de Amazon DocumentDB y conectarse a ellos cuando Amazon DocumentDB y AWS CloudShell están disponibles.
>
> - Si desea crear clústeres elásticos de Amazon DocumentDB y conectarse a ellos, consulte Introducción a los clústeres elásticos de Amazon DocumentDB.
> - Si se encuentra en las regiones de China de AWS, consulte Connect Amazon EC2 automáticamente.

Temas

- Requisitos previos
- Paso 1: creación de un clúster
- Paso 2: Conexión al clúster
- Paso 3: insertar y consultar datos
- Paso 4: explorar

Requisitos previos

Antes de crear el primer clúster de Amazon DocumentDB, debe hacer lo siguiente:

Creación de una cuenta de Amazon Web Services (AWS)

Para empezar a utilizar Amazon DocumentDB, debe tener una cuenta de Amazon Web Services (AWS). La cuenta de AWS es gratuita. Solo se paga por los servicios y los recursos que se utilicen.

Si no dispone de una Cuenta de AWS, siga estos pasos para crear una.

Procedimiento para registrarse en Cuenta de AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga las instrucciones que se le indiquen.

   Parte del procedimiento de registro consiste en recibir una llamada telefónica o mensaje de texto e indicar un código de verificación en el teclado del teléfono.

   Al registrarse en una Cuenta de AWS, se crea un Usuario raíz de la cuenta de AWS. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario y utilice únicamente el usuario raíz para realizar tareas que requieren acceso de usuario raíz.

Configure los permisos de AWS Identity and Access Management (IAM) necesarios.

El acceso para administrar los recursos de Amazon DocumentDB como clústeres, instancias y grupos de parámetros de clúster requiere credenciales que AWS puede utilizar para autenticar las solicitudes. Para obtener más información, consulte Identity and Access Management para Amazon DocumentDB.

1. En la barra de búsqueda de la Consola de administración de AWS, escriba IAM y seleccione IAM en el menú desplegable que aparece.
2. Cuando esté en la consola de IAM, seleccione Usuarios en el panel de navegación.
3. Seleccione su nombre de usuario.
4. Haga clic en Add Permission (Agregar permiso).
5. Seleccione Adjuntar políticas directamente.
6. Escriba `AmazonDocDBFullAccess` en la barra de búsqueda y selecciónelo en cuanto aparezca en los resultados de búsqueda.
7. Haga clic en Next (Siguiente).

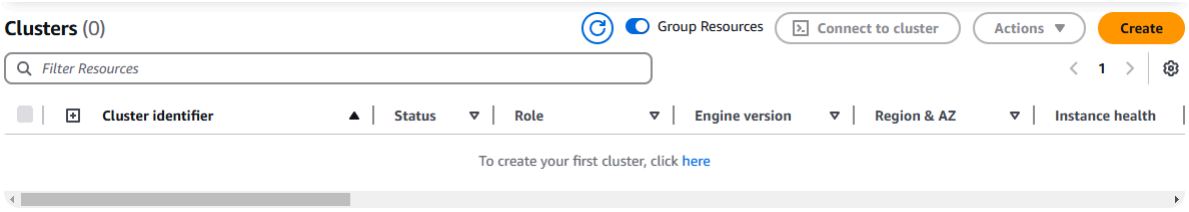
8. Haga clic en Add Permission (Agregar permiso).

> **Note**
>
> La cuenta de AWS contiene una VPC predeterminada en cada región. Si decide utilizar una Amazon VPC, complete los pasos del tema Creación de una Amazon VPC en la Guía del usuario de Amazon VPC.

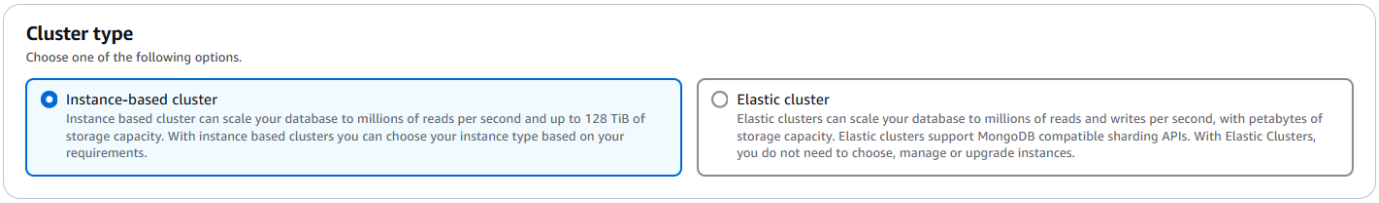
Paso 1: creación de un clúster

En este paso creará un clúster de Amazon DocumentDB.

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon DocumentDB en https://console.aws.amazon.com/docdb.
2. En la consola de administración de Amazon DocumentDB, en Clústeres, elija Crear.



3. En la página Crear clúster de Amazon DocumentDB, en la sección Tipo de clúster, elija Clúster basado en instancias (esta es la opción predeterminada).

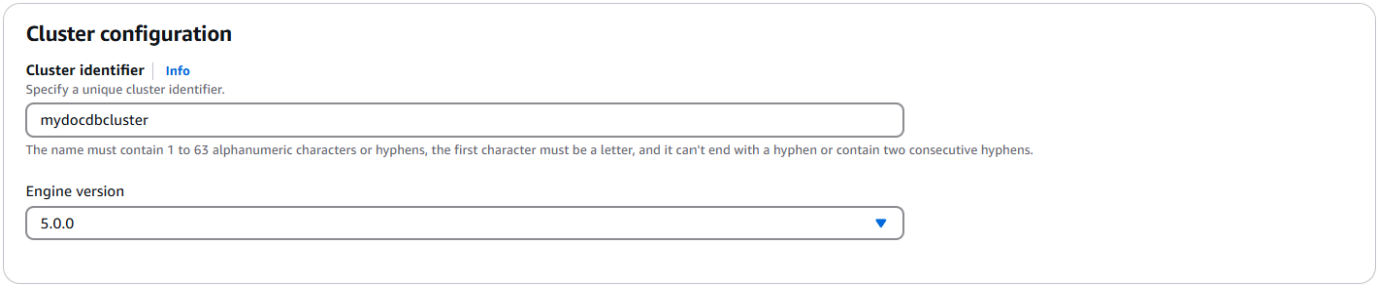


> **Note**
>
> La otra opción de esta categoría es el clúster elástico. Para obtener más información sobre los clústeres elásticos de Amazon DocumentDB, consulte Uso de Amazon DocumentDB Elastic Clusters.

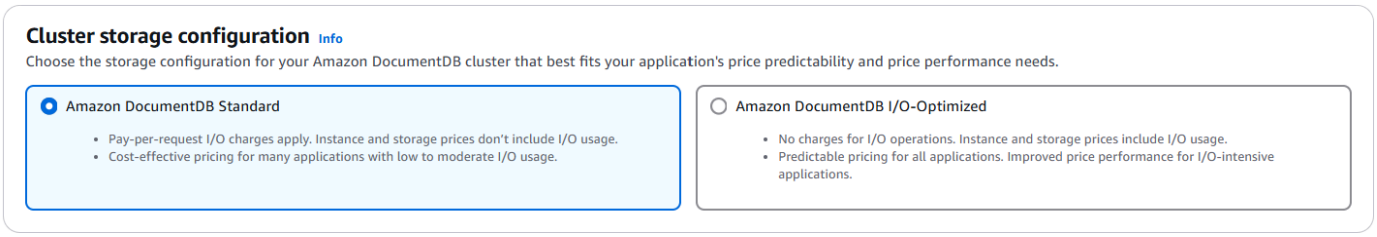
4. En la sección Configuración de clúster:

a. En el campo Identificador del clúster, ingrese un nombre único, como **`mydocdbcluster`**. Tenga en cuenta que la consola cambiará todos los nombres de los clústeres a minúsculas independientemente de cómo se ingresen.

b. En Versión del motor, elija 5.0.0.



5. En la sección Configuración del almacenamiento en clúster, elija Amazon DocumentDB estándar (es la opción predeterminada).



> **Note**
>
> La otra opción de esta categoría es Amazon DocumentDB optimizado para E/S. Para obtener más información sobre las opciones, consulte Configuraciones de almacenamiento en clústeres de Amazon DocumentDB.

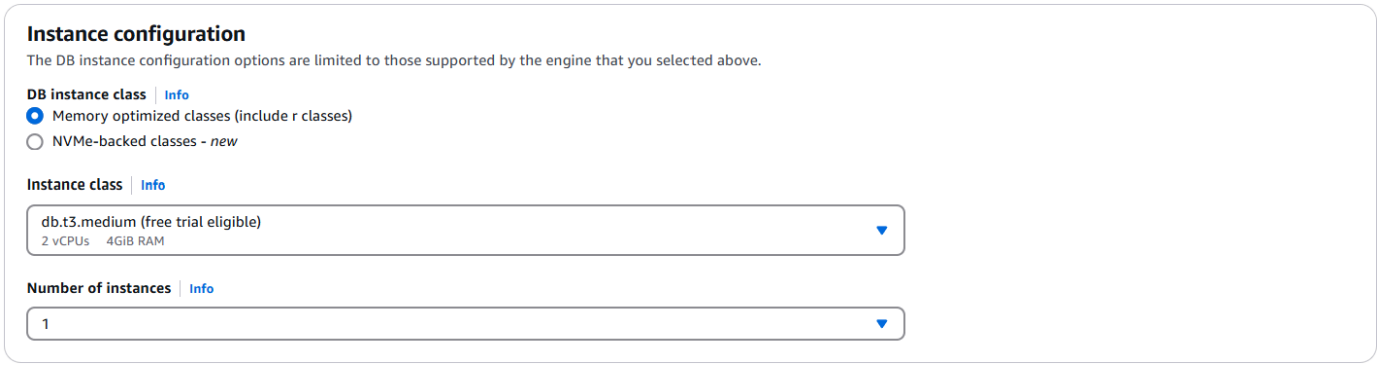
6. Sección de Configuración de instancias:

a. En Clase de instancia de base de datos, elija Clases optimizadas para memoria (incluidas las clases r), que es la opción predeterminada.

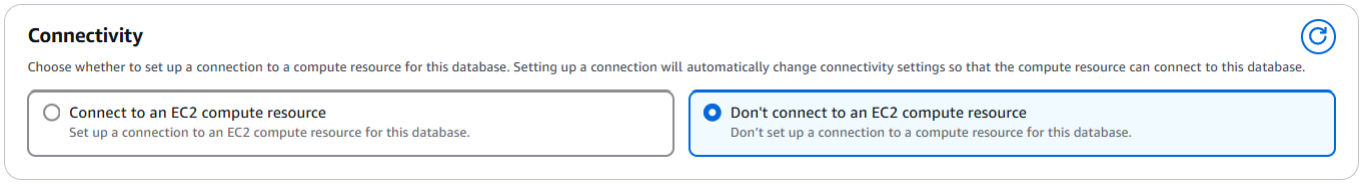
La otra opción de instancia es Clases respaldadas por NVMe. Para obtener más información, consulte Instancias respaldadas por NVMe.

b. En Clase de instancia, elija db.t3.medium. Esto es apto para la prueba gratuita de AWS.

c. En Número de instancias, elija 1 instancia. La elección de una instancia ayuda a minimizar los costos. Si se tratara de un sistema de producción, le recomendamos que aprovisione tres instancias para una alta disponibilidad.

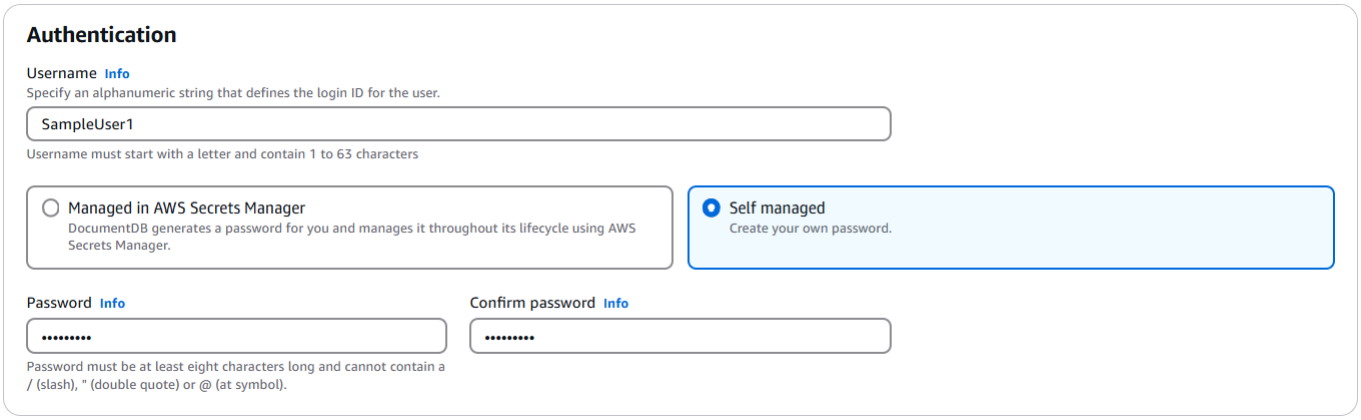


7. En la sección Conectividad, deje la configuración predeterminada de No conectarse a un recurso de computación de EC2.



8. En la sección Autenticación, ingrese un nombre de usuario para el usuario principal y, a continuación, elija Autoadministrado. Ingrese una contraseña y, a continuación, confírmela.

   Si, en su lugar, eligió Administrado en AWS Secrets Manager, consulte Administración de contraseñas con Amazon DocumentDB y AWS Secrets Manager para obtener más información.



9. Deje todas las demás opciones en sus valores predeterminados y seleccione Crear clúster.

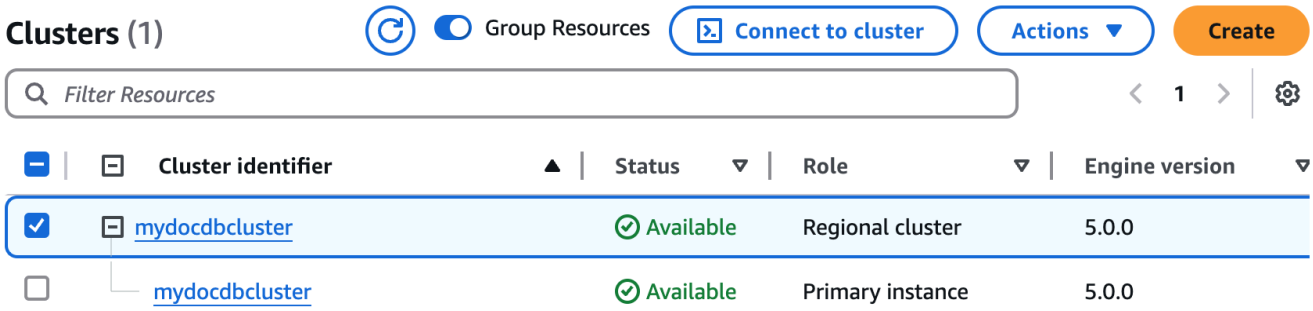
Amazon DocumentDB está aprovisionando su clúster, lo que puede tardar unos minutos en terminar.

> **Note**
>
> Para obtener información sobre los valores de estado de los clústeres, consulte Valores de estado del clúster en el capítulo Cómo monitorizar Amazon DocumentDB.

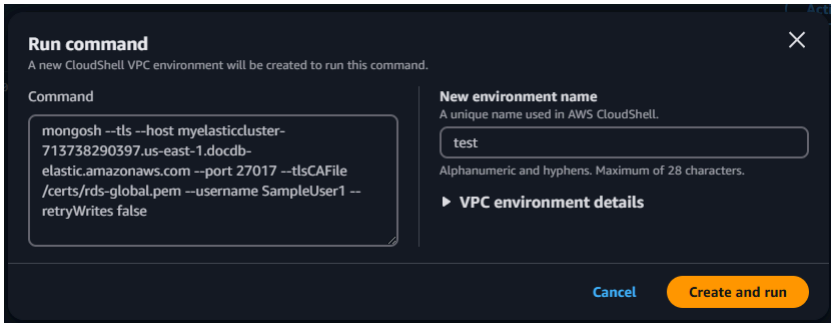
Paso 2: Conexión al clúster

Conéctese al clúster de Amazon DocumentDB mediante AWS CloudShell.

1. En la consola de administración de Amazon DocumentDB, en Clústeres, localice el clúster que ha creado. Para elegir el clúster, haga clic en la casilla de verificación situada junto a él.



2. Haga clic en Conectar al clúster (que se encuentra junto al menú desplegable Acciones). Este botón se activa solamente después de haber hecho clic en la casilla de verificación situada junto al clúster, y el estado del clúster regional y las instancias principales se muestra como Disponible. Aparece la pantalla Ejecutar comando de CloudShell.
3. En el campo Nombre del nuevo entorno, ingrese un nombre único, como «prueba» y elija Crear y ejecutar. Los detalles del entorno de la VPC se configuran automáticamente para la base de datos de Amazon DocumentDB.



4. Cuando vea la petición, introduzca la contraseña que creó en el Paso 1: crear un clúster de Amazon DocumentDB (subpaso 7).



Después de ingresar la contraseña, cuando la petición se convierte en `rs0 [direct: primary] <env-name>>`, significa que se ha conectado correctamente al clúster de Amazon DocumentDB.

> **Note**
>
> Para obtener información sobre la solución de problemas, consulte Solución de problemas de Amazon DocumentDB.

Paso 3: insertar y consultar datos

Ahora que está conectado a su clúster, puede realizar algunas consultas para familiarizarse con el uso de una base de datos de documentos.

1. Para insertar un solo documento, escriba lo siguiente:

   ```
   db.collection.insertOne({"hello":"DocumentDB"})
   ```

   Obtiene el siguiente resultado:

   ```
   {
     acknowledged: true,
     insertedId: ObjectId('673657216bdf6258466b128c')
   }
   ```

2. Puede leer el documento que escribió con el comando `findOne()` (ya que solo devuelve un documento). La siguiente entrada:

```
db.collection.findOne()
```

Obtiene el siguiente resultado:

```
{ "_id" : ObjectId("5e401fe56056fda7321fbd67"), "hello" : "DocumentDB" }
```

3. Para realizar algunas consultas más, plantéese un caso de uso de perfiles de juegos. Primero, inserte algunas entradas en una colección titulada `profiles`. La siguiente entrada:

```
db.profiles.insertMany([{ _id: 1, name: 'Matt', status: 'active', level: 12, score:
 202 },
     { _id: 2, name: 'Frank', status: 'inactive', level: 2, score: 9 },
     { _id: 3, name: 'Karen', status: 'active', level: 7, score: 87 },
     { _id: 4, name: 'Katie', status: 'active', level: 3, score: 27 }
])
```

Obtiene el siguiente resultado:

```
{ acknowledged: true, insertedIds: { '0': 1, '1': 2, '2': 3, '3': 4 } }
```

4. Utilice el comando `find()` para devolver todos los documentos de la colección de perfiles. La siguiente entrada:

```
db.profiles.find()
```

Obtendrá un resultado que coincidirá con los datos que escribió en el paso 3.

5. Utilice una consulta para un único documento mediante un filtro. La siguiente entrada:

```
db.profiles.find({name: "Katie"})
```

Obtiene el siguiente resultado:

```
{ "_id" : 4, "name" : "Katie", "status": "active", "level": 3, "score":27}
```

6. Ahora intentemos buscar un perfil y modificarlo con el comando `findAndModify`. Le daremos al usuario Matt 10 puntos adicionales con el siguiente código:

```
db.profiles.findAndModify({
```

```
        query: { name: "Matt", status: "active"},
        update: { $inc: { score: 10 } }
    })
```

Se obtiene el siguiente resultado (tenga en cuenta que la puntuación aún no ha aumentado):

```
{
    [{_id : 1, name : 'Matt', status: 'active', level: 12, score: 202}]
```

7. Puede comprobar que su puntuación ha cambiado con la siguiente consulta:

   ```
   db.profiles.find({name: "Matt"})
   ```

   Obtiene el siguiente resultado:

   ```
   { "_id" : 1, "name" : "Matt", "status" : "active", "level" : 12, "score" : 212 }
   ```

Paso 4: explorar

¡Enhorabuena! Ha completado correctamente la Guía de introducción a clústeres basados en instancias de Amazon DocumentDB.

Pasos siguientes Descubra cómo aprovechar al máximo esta base de datos con algunas de sus características más populares:

- Administración de Amazon DocumentDB
- Escalado
- Copia de seguridad y restauración

> **Note**
>
> El clúster que creó a partir de este ejercicio de introducción seguirá acumulando costos a menos que lo elimine. Para obtener instrucciones, consulte Cómo eliminar un clúster de Amazon DocumentDB.

Inicio rápido de Amazon DocumentDB con CloudFormation

Esta sección contiene pasos y otra información que le ayudarán a comenzar rápidamente a utilizar Amazon DocumentDB (compatible con MongoDB) mediante CloudFormation. Para obtener información general acerca de Amazon DocumentDB, consulte Qué es Amazon DocumentDB (compatible con MongoDB).

Estas instrucciones utilizan una AWS CloudFormation plantilla para crear un clúster e instancias en tu Amazon VPC predeterminada. Para obtener instrucciones sobre cómo crear estos recursos usted mismo, consulte Introducción a Amazon DocumentDB.

> **Important**
>
> La CloudFormation pila que crea esta plantilla crea varios recursos, incluidos los recursos de Amazon DocumentDB (por ejemplo, un clúster e instancias) y Amazon Elastic Compute Cloud (por ejemplo, un grupo de subredes).
> Algunos de estos recursos no se incluyen en la capa gratuita. Para obtener información sobre precios, consulte Amazon DocumentDB Pricing y Amazon EC2 Pricing. Puede eliminar la pila cuando haya terminado de utilizarla para suspender todos los cargos.

Esta CloudFormation pila está destinada únicamente a fines tutoriales. Si utiliza esta plantilla para un entorno de producción, le recomendamos que utilice políticas de IAM y seguridad más estrictas. Para obtener información sobre cómo proteger los recursos, consulte Amazon VPC Security y Amazon EC2 Network and Security.

Temas

- Requisitos previos
- Lanzamiento de una pila de CloudFormation de Amazon DocumentDB
- Acceso al clúster de Amazon DocumentDB
- Protección de terminación y protección de eliminación

Requisitos previos

Antes de crear un clúster de Amazon DocumentDB, debe hacer lo siguiente:

- Una VPC predeterminada de Amazon
- Los permisos necesarios de IAM

Permisos de IAM necesarios

Los siguientes permisos permiten crear recursos para la pila de CloudFormation :

AWS Políticas administradas

- `AWSCloudFormationReadOnlyAccess`
- `AmazonDocDBFullAccess`

Permisos de IAM adicionales

La siguiente política describe los permisos adicionales que se requieren para crear y eliminar esta CloudFormation pila.

En los ejemplos siguientes, sustituya cada uno *`user input placeholder`* por la información de su recurso.

Par de EC2 claves de Amazon

Debe tener un par de claves (y el archivo PEM) disponibles en la región en la que va a crear la CloudFormation pila. Si necesitas crear un par de claves, consulta Cómo crear un par de claves con Amazon EC2 en la Guía del EC2 usuario de Amazon.

Lanzamiento de una pila de CloudFormation de Amazon DocumentDB

En esta sección se describe cómo lanzar y configurar una pila CloudFormation de Amazon DocumentDB.

1. Inicia sesión Consola de administración de AWS enhttps://console.aws.amazon.com/.
2. En la tabla siguiente se muestran las plantillas de pilas de Amazon DocumentDB para cada Región de AWS. Elige Launch Stack para la pila en la que Región de AWS deseas lanzar tu stack.

Region	Ver plantilla	Ver en Designer	Lanzar
Este de EE. UU. (Ohio)	Ver plantilla	Ver en Designer	Launch Stack
Este de EE. UU. (Norte de Virginia)	Ver plantilla	Ver en Designer	Launch Stack
Oeste de EE. UU. (Oregón)	Ver plantilla	Ver en Designer	Launch Stack
Asia-Pacífico (Mumbai)	Ver plantilla	Ver en Designer	Launch Stack
Asia-Pacífico (Seúl)	Ver plantilla	Ver en Designer	Launch Stack
Asia-Pacífico (Singapur)	Ver plantilla	Ver en Designer	Launch Stack
Asia-Pacífico (Sídney)	Ver plantilla	Ver en Designer	Launch Stack
Asia-Pacífico (Tokio)	Ver plantilla	Ver en Designer	Launch Stack
Canadá (centro)	Ver plantilla	Ver en Designer	Launch Stack
Europa (Fráncfort)	Ver plantilla	Ver en Designer	Launch Stack
Europa (Irlanda)	Ver plantilla	Ver en Designer	Launch Stack
Europa (Londres)	Ver plantilla	Ver en Designer	Launch Stack
Europa (París)	Ver plantilla	Ver en Designer	Launch Stack

3. Crear pila: describe la plantilla de Amazon DocumentDB que ha seleccionado. Cada pila se basa en una plantilla (un archivo JSON o YAML) que contiene la configuración de los AWS recursos que quieres incluir en la pila. Como eligió lanzar una pila a partir de las plantillas proporcionadas anteriormente, su plantilla ya se configuró para crear una pila de Amazon DocumentDB para la Región de AWS que eligió.

   Al lanzar una CloudFormation pila, la protección contra la eliminación del clúster de Amazon DocumentDB está deshabilitada de forma predeterminada. Si desea habilitar la protección de eliminación para el clúster, complete los pasos siguientes. De lo contrario, elija Next (Siguiente) para continuar con el paso siguiente.

   Para habilitar la protección de eliminación para el clúster de Amazon DocumentDB:

   1. Elija View in Designer (Ver en Designer) en la esquina inferior derecha de la página Create stack (Crear pila).
   2. Modifique la plantilla mediante el editor JSON y YAML integrado en la página de CloudFormation diseño resultante de la consola. Desplácese hasta la sección `Resources` y modifíquela para incluir `DeletionProtection`, de la siguiente manera. Para obtener más información sobre el uso de CloudFormation Designer, consulte ¿Qué es el CloudFormation diseñador? .

      JSON:

```
"Resources": {
    "DBCluster": {
        "Type": "AWS::DocDB::DBCluster",
        "DeletionPolicy": "Delete",
        "Properties": {
            "DBClusterIdentifier": {
                "Ref": "DBClusterName"
            },
            "MasterUsername": {
                "Ref": "MasterUser"
            },
            "MasterUserPassword": {
                "Ref": "MasterPassword"
            },
            "DeletionProtection": "true"
        }
    },
```

YAML:

```
Resources:
  DBCluster:
    Type: 'AWS::DocDB::DBCluster'
    DeletionPolicy: Delete
    Properties:
      DBClusterIdentifier: !Ref DBClusterName
      MasterUsername: !Ref MasterUser
      MasterUserPassword: !Ref MasterPassword
      DeletionProtection: 'true'
```

3. Elija Create stack (Crear pila)

   ()

   en la esquina superior izquierda de la página para guardar los cambios y crear una pila con estos cambios habilitados.

4. Después de guardar los cambios, se le redirigirá a la página Create stack (Crear pila).

5. Elija Siguiente para continuar.

4. Especificar los detalles de la pila: introduce el nombre y los parámetros de la pila de su plantilla. Los parámetros se definen en la plantilla y le permiten ingresar valores personalizados al crear o actualizar una pila.

   - En Stack name (Nombre de la pila), escriba un nombre para su pila o acepte el nombre proporcionado. El nombre de la pila puede incluir letras (A-Z y a-z), números (0-9) y guiones (-).
   - En Parameters (Parámetros), escriba los siguientes detalles:

     - DBClusterNombre: introduzca un nombre para el clúster de Amazon DocumentDB o acepte el nombre proporcionado.

       Restricciones en cuanto a la nomenclatura de los clústeres:

       - Debe tener [1-63] letras, números o guiones.
       - El primer carácter debe ser una letra.
       - No puede terminar con un guion ni contener dos guiones consecutivos.
       - Debe ser único para todos los clústeres de Amazon RDS, Neptune y Amazon DocumentDB por región. Cuenta de AWS

- DBInstanceClase: en la lista desplegable, seleccione la clase de instancia para su clúster de Amazon DocumentDB.
- DBInstanceNombre: introduzca un nombre para su instancia de Amazon DocumentDB o acepte el nombre proporcionado.

  Restricciones en cuanto a la nomenclatura de las instancias:

  - Debe tener [1-63] letras, números o guiones.
  - El primer carácter debe ser una letra.
  - No puede terminar con un guion ni contener dos guiones consecutivos.
  - Debe ser único para todas las instancias de Amazon RDS, Neptune y Amazon DocumentDB por región. Cuenta de AWS
- MasterPassword— La contraseña de la cuenta de administrador de la base de datos.
- MasterUser— El nombre de usuario de la cuenta de administrador de base de datos. MasterUser Debe empezar por una letra y solo puede contener caracteres alfanuméricos.

Elija Next (Siguiente) para guardar los cambios y continuar.

5. Configure opciones de pila: configure las etiquetas, los permisos y las opciones adicionales de su pila.

   - Etiquetas: especifique los pares de etiquetas (clave-valor) para aplicarlos a los recursos de su pila. Puede agregar hasta 50 etiquetas únicas para cada pila.
   - Permisos: opcionales. Elija una función de IAM para definir de forma explícita cómo CloudFormation se pueden crear, modificar o eliminar los recursos de la pila. Si no elige un rol, CloudFormation utiliza los permisos en función de sus credenciales de usuario. Antes de especificar un rol de servicio, asegúrese de que tiene permiso para pasarlo (`iam:PassRole`). El permiso `iam:PassRole` especifica los roles que puede utilizar.

     > **Note**
     >
     > Cuando especificas un rol de servicio, CloudFormation siempre lo usa para todas las operaciones que se realizan en esa pila. Otros usuarios con permisos para realizar operaciones en esta pila podrán utilizar este rol, aunque no tengan permiso para pasarlo. Si el rol incluye permisos que el usuario no debería tener, puede escalar involuntariamente los permisos de un usuario. Asegúrese de que el rol concede privilegios mínimos.

- Opciones avanzadas: puede definir las siguientes opciones avanzadas:
  - Política de pilas: opcional. Define los recursos que desea proteger de actualizaciones involuntarias durante una actualización de pila. De forma predeterminada, se pueden actualizar todos los recursos durante una actualización de pila.

    Puede introducir la política de pilas directamente como JSON o cargar un archivo JSON que contenga la política de pilas. Para obtener más información, consulte Evitar actualizaciones en los recursos de la pila.
  - Configuración de reversión: opcional. Especifique las alarmas de CloudWatch registro CloudFormation que desee supervisar al crear y actualizar la pila. Si la operación supera un umbral de alarma, CloudFormation lo revierte.
  - Opciones de notificación: opcional. Especifique los temas para el sistema de notificación simple (SNS).
  - Opciones de creación de la pila: opcional. Puede especificar las opciones siguientes:
    - Restauración en caso de error: si la pila se debería restaurar o no en caso de error de creación de la pila.
    - Tiempo de espera: se han agotado los minutos de espera de la creación de la pila.
    - Protección de terminación: impide que se elimine una pila accidentalmente.

      > **Note**
      >
      > CloudFormation la protección de rescisión es diferente del concepto de protección de eliminación de Amazon DocumentDB. Para obtener más información, consulte Protección de terminación y protección de eliminación.

Elija Siguiente para continuar.

6. Revisar <stack-name>: revise la plantilla, los detalles y las opciones de configuración de la pila. También puede abrir un quick-create link (enlace de creación rápida) en la parte inferior de la página para crear pilas con las mismas configuraciones básicas que esta.

   - Elija Create (Crear) para crear la pila.
   - De forma alternativa, puede elegir Create change set (Crear conjunto de cambios). Un conjunto de cambios es una vista previa de cómo se configurará esta pila antes de crear la pila. Esto le permite examinar varias configuraciones antes de ejecutar el conjunto de cambios.

Acceso al clúster de Amazon DocumentDB

Una vez completada la CloudFormation pila, puede usar una EC2 instancia de Amazon para conectarse a su clúster de Amazon DocumentDB. Para obtener información sobre cómo conectarse a una EC2 instancia de Amazon mediante SSH, consulte Connect to Your Linux Instance en la Guía del EC2 usuario de Amazon.

Una vez conectado, consulte las siguientes secciones que contienen información sobre cómo usar Amazon DocumentDB.

- Paso 3: insertar y consultar datos
- Administración de recursos de Amazon DocumentDB
- Monitorización de Amazon DocumentDB

Protección de terminación y protección de eliminación

Una de las mejores prácticas de Amazon DocumentDB es habilitar la protección contra la eliminación y la protección contra la terminación. CloudFormation la protección por rescisión es una característica claramente diferente de la función de protección contra eliminaciones de Amazon DocumentDB.

- Protección de terminación: puede evitar que una pila se elimine accidentalmente activando la protección de terminación para su CloudFormation pila. Si un usuario intenta eliminar una pila con protección de terminación habilitada en ella, la eliminación falla y la pila no cambia. La protección de terminación está desactivada de forma predeterminada al crear una pila utilizando CloudFormation. Es posible habilitar la protección de terminación en una pila al crearla. Para obtener más información, consulte Configuración de las opciones de CloudFormation pila.
- Protección de eliminación: Amazon DocumentDB también ofrece la posibilidad de habilitar la protección contra la eliminación de un clúster. Si un usuario intenta eliminar un clúster de Amazon DocumentDB con la protección de eliminación habilitada en él, la eliminación falla y el clúster permanece sin cambios. La protección de eliminación, cuando está habilitada, protege contra eliminaciones accidentales de Amazon Consola de administración de AWS DocumentDB AWS CLI, y. CloudFormation Para obtener más información sobre cómo habilitar y deshabilitar la protección de eliminación para un clúster de Amazon DocumentDB, consulte Protección contra eliminación.

Compatibilidad de Amazon DocumentDB con MongoDB

Amazon DocumentDB admite la compatibilidad con MongoDB, incluidos MongoDB 4.0, MongoDB 5.0 y MongoDB 8.0. La compatibilidad con MongoDB significa que la gran mayoría de las aplicaciones, controladores y herramientas que ya utiliza en la actualidad con sus bases de datos de MongoDB se pueden utilizar con Amazon DocumentDB con pocos o ningún cambio. En esta sección se describe todo lo que necesita saber sobre la compatibilidad de Amazon DocumentDB con MongoDB, incluyendo las nuevas capacidades y características, los primeros pasos, las rutas de migración y las diferencias funcionales.

Temas

- Compatibilidad con MongoDB 8.0
- Compatibilidad con MongoDB 5.0
- Compatibilidad con MongoDB 4.0

Compatibilidad con MongoDB 8.0

Temas

- Novedades de Amazon DocumentDB 8.0
- Comience a utilizar Amazon DocumentDB 8.0
- Actualización o migración a Amazon DocumentDB 5.0 u 8.0
- Diferencias funcionales

Novedades de Amazon DocumentDB 8.0

Amazon DocumentDB 8.0 mejora el rendimiento de las consultas hasta 7 veces y mejora la relación de compresión hasta 5 veces, lo que le permite crear aplicaciones de alto rendimiento a un costo menor. Amazon DocumentDB 8.0 es totalmente compatible con el protocolo de cable con MongoDB 8.0. El siguiente resumen presenta algunas de las principales características que se introdujeron en Amazon DocumentDB 8.0. Para ver una lista completa de nuevas capacidades, consulte Notas de la versión.

- Proporciona compatibilidad con MongoDB 8.0 al agregar soporte para los controladores de API de MongoDB 8.0. También es compatible con aplicaciones que se crean con las versiones 6.0 y 7.0 de la API de MongoDB.
- El nuevo planificador de consultas de Amazon DocumentDB 8.0 amplía las mejoras de rendimiento a los operadores de las etapas de agregación, además de admitir optimizaciones de la canalización de agregación y comandos distintos.
- Amazon DocumentDB 8.0 admite la intercalación y las vistas.
- Ofrece 6 nuevas etapas de agregación: $replaceWith, $VectorSearch, $merge, $set, $unset, $bucket y 3 nuevos operadores de agregación $pow, $rand y $dateTrunc.
- Una nueva versión del índice de texto: el índice de texto v2 de Amazon DocumentDB 8.0 incorpora tokens adicionales, lo que mejora las capacidades de búsqueda de texto.
- Mediante la creación de índices vectoriales paralelos, Amazon DocumentDB 8.0 reduce el tiempo de creación de índices hasta 30 veces.

Comience a utilizar Amazon DocumentDB 8.0

Para empezar a utilizar Amazon DocumentDB 8.0, consulte la Guía de introducción. Puede crear un nuevo clúster de Amazon DocumentDB 8.0 mediante el AWS SDK AWS CLI, Consola de administración de AWS o. CloudFormation Al conectarse a Amazon DocumentDB, es necesario que utilice un controlador o una utilidad de MongoDB que sea compatible con MongoDB 5.0 o superior.

> **Note**
>
> Cuando utilice el AWS SDK o el motor CloudFormation, la versión predeterminada será 5.0.0. AWS CLI Debe especificar explícitamente el parámetro `engineVersion = 8.0.0` para crear un nuevo clúster de Amazon DocumentDB 8.0 o `engineVersion = 4.0.0` para crear un nuevo clúster de Amazon DocumentDB 4.0 `engineVersion = 3.6.0` o para crear un nuevo clúster de Amazon DocumentDB 3.6. Para un clúster de Amazon DocumentDB determinado, puede determinar la versión del clúster mediante la llamada `describe-db-clusters` o AWS CLI utilizar la consola de administración de Amazon DocumentDB para ver el número de versión del motor de un clúster en particular.

Amazon DocumentDB 5.0 es compatible con los procesadores Amazon EC2 `r8g` Graviton4 y Graviton2, así como los tipos de `t4.medium` instancia para sus clústeres, `r6g` y está disponible

en todas las regiones compatibles (consulte). instancias Para obtener más información acerca del precio, consulte Amazon DocumentDB (with MongoDB compatibility) Pricing.

Actualización o migración a Amazon DocumentDB 5.0 u 8.0

Puede migrar de MongoDB 3.6 o MongoDB 4.0 a Amazon DocumentDB 5.0 o Amazon DocumentDB 8.0 mediante utilidades como,, y. AWS DMS`mongodump` `mongorestore` `mongoimport` `mongoexport` Para obtener instrucciones sobre cómo migrar, consulte Actualización del clúster de Amazon DocumentDB mediante AWS Database Migration Service.

Diferencias funcionales

Diferencias funcionales entre Amazon DocumentDB 5.0 y 8.0

Con el lanzamiento de Amazon DocumentDB 8.0, existen diferencias funcionales entre Amazon DocumentDB 5.0 y Amazon DocumentDB 8.0:

- Planner v1 es el planificador de consultas predeterminado en Amazon DocumentDB 5.0, mientras que el Planner v3, de mayor rendimiento, es el predeterminado en Amazon DocumentDB 8.0.
- Las nuevas funciones de Amazon DocumentDB 8.0, incluidas las vistas, la intercalación y operadores como $merge, solo son compatibles con Planner v3.
- La compresión está activada de forma predeterminada en Amazon DocumentDB 8.0 y está configurada para usar el algoritmo Zstandard. Además, en Amazon DocumentDB 8.0, «activado» ya no es una opción válida; puede seleccionar entre Zstd y ninguna. LZ4
- Las capacidades más recientes de Amazon DocumentDB 5.0, incluidas las instancias R8g y sin servidor, no están disponibles actualmente en Amazon DocumentDB 8.0.

Compatibilidad con MongoDB 5.0

Temas

- Novedades de Amazon DocumentDB 5.0
- Introducción a Amazon DocumentDB 5.0
- Actualización o migración a Amazon DocumentDB 5.0
- Diferencias funcionales

Novedades de Amazon DocumentDB 5.0

Amazon DocumentDB 5.0 presenta nuevas características y capacidades que incluyen límites de almacenamiento y cifrado a nivel de campo del lado del cliente. El siguiente resumen presenta algunas de las principales características que se introdujeron en Amazon DocumentDB 5.0. Para ver una lista completa de nuevas capacidades, consulte Notas de la versión.

- Se aumentó el límite de almacenamiento a 128 TiB para los clústeres de Amazon DocumentDB basados en instancias y para los clústeres elásticos basados en particiones.
- Se presentó el motor Amazon DocumentDB 5.0 (versión 3.0.775)
  - Compatibilidad con los controladores API de MongoDB 5.0
  - Compatibilidad con el cifrado a nivel de campo (FLE) del lado del cliente. Ahora puede cifrar los campos del lado del cliente antes de escribir los datos en el clúster de Amazon DocumentDB. Para obtener más información, consulte Cifrado a nivel de campo del lado del cliente.
  - Nuevos operadores de agregación: `$dateAdd`, `$dateSubtract`
  - Compatibilidad con índices con operador `$elemMatch`. Como resultado, las consultas que se realicen con `$elemMatch`, darán lugar a escaneos del índice.

Amazon DocumentDB no es compatible con todas las funciones de MongoDB 5.0. Cuando creamos Amazon DocumentDB 5.0, partimos de las características y capacidades que nuestros clientes nos pedían más. Seguiremos añadiendo capacidades adicionales a MongoDB 5.0 en función de lo que nos pidan los clientes. Para obtener la lista más reciente de las compatibles, consulte. APIs APIsMongoDB, operaciones y tipos de datos compatibles en Amazon DocumentDB

Introducción a Amazon DocumentDB 5.0

Para empezar a utilizar Amazon DocumentDB 5.0, consulte la Guía de introducción. Puede crear un nuevo clúster de Amazon DocumentDB 5.0 mediante el AWS SDK AWS CLI, Consola de administración de AWS o. CloudFormation Al conectarse a Amazon DocumentDB, es necesario que utilice un controlador o una utilidad de MongoDB que sea compatible con MongoDB 5.0 o superior.

> **Note**
>
> Cuando utilice el AWS SDK o el motor CloudFormation, la versión predeterminada será 5.0.0. AWS CLI Debe especificar de forma explícita el parámetro `engineVersion = 4.0.0` para crear un nuevo clúster de Amazon DocumentDB 4.0 o `engineVersion = 3.6.0` para crear un nuevo clúster de Amazon DocumentDB 3.6. Para un clúster de Amazon

DocumentDB determinado, puede determinar la versión del clúster mediante la llamada `describe-db-clusters` o AWS CLI utilizar la consola de administración de Amazon DocumentDB para ver el número de versión del motor de un clúster en particular.

Amazon DocumentDB 5.0 es compatible con los procesadores Amazon EC2 `r8g` Graviton4 y Graviton2, así como los tipos de `t4.medium` instancia para sus clústeres, `r6g` y está disponible en todas las regiones compatibles (consulte). instancias Para obtener más información acerca del precio, consulte Amazon DocumentDB (with MongoDB compatibility) Pricing.

Actualización o migración a Amazon DocumentDB 5.0

Puede migrar de MongoDB 3.6 o MongoDB 4.0 a Amazon DocumentDB 5.0 mediante AWS DMS o mediante utilidades como `mongodump`, `mongorestore`, `mongoimport`, y `mongoexport`. Para obtener instrucciones sobre cómo migrar, consulte Actualización del clúster de Amazon DocumentDB mediante AWS Database Migration Service.

Diferencias funcionales

Diferencias funcionales entre Amazon DocumentDB 4.0 y 5.0

Con el lanzamiento de Amazon DocumentDB 5.0, existen diferencias funcionales entre Amazon DocumentDB 4.0 y Amazon DocumentDB 5.0:

- La función de copia de seguridad integrada ahora es compatible con `serverStatus`. Acción: los desarrolladores y las aplicaciones con función de backup pueden recopilar estadísticas sobre el estado del clúster de Amazon DocumentDB.
- El campo `SecondaryDelaySecs` reemplaza a `slaveDelay` en la salida `replSetGetConfig`.
- El comando hello reemplaza a `isMaster` - hello devuelve un documento que describe la función de un clúster de Amazon DocumentDB.
- Amazon DocumentDB 5.0 ahora es compatible con escaneos de índices con el operador `$elemMatch` en el primer nivel de anidación. Los escaneos de índices son compatibles cuando el filtro para solo consultas tiene un nivel de filtro de `$elemMatch`, pero no son compatibles si se incluye una consulta de `$elemMatch` anidada.

  Por ejemplo, en Amazon DocumentDB 5.0, si usted incluye el operador `$elemMatch` en el nivel anidado, no devolverá un valor como lo hace en Amazon DocumentDB 4.0:

```
db.foo.insert(
[
    {a: {b: 5}},
    {a: {b: [5]}},
    {a: {b: [3, 7]}},
    {a: [{b: 5}]},
    {a: [{b: 3}, {b: 7}]},
    {a: [{b: [5]}]},
    {a: [{b: [3, 7]}]},
    {a: [[{b: 5}]]},
    {a: [[{b: 3}, {b: 7}]]},
    {a: [[{b: [5]}]]},
    {a: [[{b: [3, 7]}]]}
]);

// DocumentDB 5.0
> db.foo.find({a: {$elemMatch: {b: {$elemMatch: {$lt: 6, $gt: 4}}}}}, {_id: 0})
{ "a" : [ { "b" : [ 5 ] } ] }

// DocumentDB 4.0
> db.foo.find({a: {$elemMatch: {b: {$elemMatch: {$lt: 6, $gt: 4}}}}}, {_id: 0})
{ "a" : [ { "b" : [ 5 ] } ] }
{ "a" : [ [ { "b" : [ 5 ] } ] ] }
```

- La proyección “$” de Amazon DocumentDB 4.0 devuelve todos los documentos con todos los campos. Con Amazon DocumentDB 5.0, el comando find con una proyección “$” devuelve los documentos que coinciden con el parámetro de consulta y contienen solo el campo que coincide con la proyección “$”.
- En Amazon DocumentDB 5.0, los comandos find con parámetros de consulta `$regex` y `$options` los comandos devuelven un error: “No se pueden establecer opciones en ambos`$regex` y `$options`”.
- Con Amazon DocumentDB 5.0, `$indexOfCP` ahora devuelve “-1” cuando:
  - la subcadena no se encuentra en la expresión de cadena, o
  - el inicio es un número mayor que el final, o
  - el inicio es un número mayor que la longitud en bytes de la cadena.
- En Amazon DocumentDB 4.0, `$indexOfCP` devuelve “0” cuando la posición inicial es un número mayor que el final o que la longitud en bytes de la cadena.

- Con Amazon DocumentDB 5.0, las operaciones de proyección en `_id fields`, por ejemplo `{"_id.nestedField" : 1}`, devuelven documentos que solo incluyen el campo proyectado. En cambio, en Amazon DocumentDB 4.0, los comandos de proyección de campos anidados no filtran ningún documento.

Compatibilidad con MongoDB 4.0

Temas

- Características de Amazon DocumentDB 4.0
- Introducción a Amazon DocumentDB 4.0
- Actualización o migración a Amazon DocumentDB 4.0
- Diferencias funcionales

Características de Amazon DocumentDB 4.0

Amazon DocumentDB 4.0 introdujo muchas características y capacidades nuevas que incluían transacciones ACID y mejoras en los flujos de cambios. El siguiente resumen presenta algunas de las principales características que se introdujeron en Amazon DocumentDB 4.0. Para ver una lista completa de capacidades, consulte Notas de la versión.

- Transacciones ACID: Amazon DocumentDB ahora es compatible con la capacidad de realizar transacciones en varios documentos, estados de cuenta, colecciones y bases de datos. Las transacciones simplifican el desarrollo de aplicaciones al permitirle realizar operaciones atómicas, consistentes, aisladas y duraderas (ACID) en uno o más documentos dentro de un clúster de Amazon DocumentDB. Para obtener más información, consulte Transacciones en Amazon DocumentDB.
- Flujos de cambios: ahora puede abrir un flujo de cambios a nivel de clúster (`client.watch()` o `mongo.watch()`) y la base de datos (`db.watch()`), puede especificar un `startAtOperationTime` para abrir el cursor de flujo de cambios y, por último, puede ampliar el período de retención del flujo de cambios a 7 días (anteriormente 24 horas). Para obtener más información, consulte Uso de flujos de cambios con Amazon DocumentDB.
- AWS Database Migration Service(AWS DMS): Ahora puede usarlo AWS DMS para migrar sus cargas de trabajo de MongoDB 4.0 a Amazon DocumentDB. AWS DMS ahora admite una fuente de MongoDB 4.0, un destino de Amazon DocumentDB 4.0 y una fuente de Amazon

DocumentDB 3.6 para realizar actualizaciones entre Amazon DocumentDB 3.6 y 4.0. Para obtener más información, consulte la Documentación de AWS DMS.

- Rendimiento e indexación: puede utilizar un índice con `$lookup`, buscar consultas con una proyección que contenga un campo o un campo y el campo `_id` puede servir directamente desde el índice sin necesidad de leer la colección (consulta cubierta), capacidad de `hint()` con `findAndModify`, optimizaciones del rendimiento para `$addToSet` y mejoras para reducir el tamaño general de los índices. Para obtener más información, consulte Notas de la versión.
- Operadores: Amazon DocumentDB 4.0 ahora es compatible varios operadores de agregación nuevos: `$ifNull`, `$replaceRoot`, `$setIsSubset`, `$setIntersection`, `$setUnion`, `$setEquals`. Puede ver todos los tipos de datos, operaciones y APIs MongoDB que admitimos en. APIsMongoDB, operaciones y tipos de datos compatibles en Amazon DocumentDB
- Control de acceso basado en funciones (RBAC): con los comandos `ListCollection` y `ListDatabase`, ahora puede usar opcionalmente los parámetros `authorizedCollections` y `authorizedDatabases` para permitir a los usuarios enlistar las colecciones y bases de datos a las que tienen permiso de acceso sin necesitar las funciones `listCollections` y `listDatabase`, respectivamente. También puede eliminar sus propios cursores sin necesitar la función `KillCursor`.

Amazon DocumentDB no es compatible con todas las funciones de MongoDB 4.0. Cuando creamos Amazon DocumentDB 4.0, partimos de las características y capacidades que nuestros clientes nos pedían más. Seguiremos añadiendo capacidades adicionales a MongoDB 4.0 en función de lo que nos pidan los clientes. Por ejemplo, Amazon DocumentDB 4.0 actualmente no es compatible con los operadores de conversión de tipos ni con los operadores de cadenas que se introdujeron en MongoDB 4.0. Para ver la lista más reciente de los compatibles APIs, consulta. APIsMongoDB, operaciones y tipos de datos compatibles en Amazon DocumentDB

Introducción a Amazon DocumentDB 4.0

Para empezar a utilizar Amazon DocumentDB 4.0, consulte la Guía de introducción. Puede crear un nuevo clúster de Amazon DocumentDB 4.0 mediante el AWS SDK AWS CLI, Consola de administración de AWS o. CloudFormation Al conectarse a Amazon DocumentDB, es necesario que utilice un controlador o una utilidad de MongoDB que sea compatible con MongoDB 4.0 o superior.

> **Note**
>
> Cuando utilice el AWS SDK o el motor CloudFormation, la versión predeterminada será 5.0.0. AWS CLI Debe especificar de forma explícita el parámetro `engineVersion = 4.0.0`

para crear un nuevo clúster de Amazon DocumentDB 4.0 o `engineVersion = 3.6.0` para crear un nuevo clúster de Amazon DocumentDB 3.6. Para un clúster de Amazon DocumentDB determinado, puede determinar la versión del clúster mediante la llamada `describe-db-clusters` o AWS CLI utilizar la consola de administración de Amazon DocumentDB para ver el número de versión del motor de un clúster en particular.

Amazon DocumentDB 4.0 es compatible con los tipos de instancia `r5`, `r6g`, `t3.medium` y `t4g.medium` para sus clústeres y está disponible en todas las regiones compatibles. La utilización de Amazon DocumentDB 4.0 no implica costos adicionales. Para obtener más información acerca del precio, consulte Amazon DocumentDB (with MongoDB compatibility) Pricing.

Actualización o migración a Amazon DocumentDB 4.0

Puede migrar de MongoDB 3.6 o de MongoDB 4.0 a Amazon DocumentDB 4.0 mediante AWS DMS o de utilidades como `mongodump`, `mongorestore`, `mongoimport` y `mongoexport`. De forma similar, puede utilizar las mismas herramientas para actualizar de Amazon DocumentDB 3.6 a Amazon DocumentDB 4.0. Para obtener instrucciones sobre cómo migrar, consulte Actualización del clúster de Amazon DocumentDB mediante AWS Database Migration Service.

Diferencias funcionales

Diferencias funcionales entre Amazon DocumentDB 3.6 y 4.0

Con el lanzamiento de Amazon DocumentDB 4.0, existen diferencias funcionales entre Amazon DocumentDB 3.6 y Amazon DocumentDB 4.0:

- Proyección para documentos anidados: Amazon DocumentDB 3.6 considera el primer campo de un documento anidado al aplicar una proyección. Sin embargo, Amazon DocumentDB 4.0 analizará los subdocumentos y aplicará la proyección a cada uno de ellos. Por ejemplo: si la proyección lo es `"a.b.c": 1`, el comportamiento en ambas versiones es idéntico. Sin embargo, si la proyección es `{a:{b:{c:1}}}`, Amazon DocumentDB 3.6 solo aplicará la proyección a “a” y no a “b” o “c”.
- Comportamiento de **`minKey`**, **`maxKey`**: con Amazon DocumentDB 4.0, el comportamiento de `{x:{$gt:MaxKey}}` no devuelve nada y para `{x:{$lt:MaxKey}}`, lo devuelve todo.
- Diferencias en la comparación de documentos: la comparación de valores numéricos de distintos tipos (doble, int, long) en subdocumentos (p. ej., b en `{"_id" :1, "a" :{"b":1}}`) ahora

proporciona un resultado coherente en todos los tipos de datos numéricos y para cada nivel de un documento.

Diferencias funcionales entre Amazon DocumentDB 4.0 y MongoDB 4.0

A continuación, se muestran las diferencias funcionales entre Amazon DocumentDB 4.0 y MongoDB 4.0.

- Búsqueda de una clave vacía en la ruta: cuando una colección contiene un documento con una clave vacía dentro de la matriz (por ejemplo `{"x" : [ { "" : 10 }, { "b" : 20 } ]}`) y cuando la clave utilizada en la consulta termina en una cadena vacía (por ejemplo `x.`), Amazon DocumentDB devolverá ese documento, ya que recorre todos los documentos de la matriz, mientras que MongoDB no lo devolverá.
- **`$setOnInsert`** junto con **`$`** en la ruta: el operador de campo `$setOnInsert` no funcionará en combinación con $ en la ruta en Amazon DocumentDB, lo que también es coherente con MongoDB 4.0.

Transacciones en Amazon DocumentDB

Amazon DocumentDB (con compatibilidad con MongoDB) admite ahora la compatibilidad con MongoDB 4.0, incluidas las transacciones. Puede realizar transacciones en varios documentos, estados de cuenta, colecciones y bases de datos. Las transacciones simplifican el desarrollo de aplicaciones al permitirle realizar operaciones atómicas, consistentes, aisladas y duraderas (ACID) en uno o más documentos dentro de un clúster de Amazon DocumentDB. Los casos de uso más comunes de las transacciones incluyen el procesamiento financiero, el cumplimiento y la gestión de pedidos y la creación de juegos para varios jugadores.

No hay ningún costo adicional para las transacciones. Solo paga por los dispositivos iOS de lectura y escritura que consuma como parte de las transacciones.

Temas

- Requisitos
- Prácticas recomendadas
- Limitaciones
- Supervisión y diagnóstico
- Nivel de aislamiento de transacciones
- Casos de uso
- Comandos admitidos
- Capacidades no compatibles
- Sesiones
- Errores de la transacción

Requisitos

Para utilizar la función de transacciones, debe cumplir los siguientes requisitos:

- Debe utilizar el motor Amazon DocumentDB 4.0.
- Debe utilizar un controlador compatible con MongoDB 4.0 o superior.

Prácticas recomendadas

Estas son algunas de las prácticas recomendadas para que pueda aprovechar al máximo las transacciones con Amazon DocumentDB.

- Confirme o cancele siempre la transacción una vez que se haya completado. Dejar una transacción incompleta agota los recursos de la base de datos y puede provocar conflictos de escritura.
- Se recomienda limitar las transacciones al menor número de comandos necesario. Si tiene transacciones con varios estados de cuenta que se pueden dividir en varias transacciones más pequeñas, es recomendable hacerlo para reducir la probabilidad de que se agote el tiempo de espera. Procure siempre de crear transacciones cortas, no lecturas prolongadas.

Limitaciones

- Amazon DocumentDB no admite cursores en una transacción.
- Amazon DocumentDB no puede crear nuevas colecciones en una transacción ni realizar consultas ni actualizar colecciones no existentes.
- Los bloqueos de escritura a nivel de documento están sujetos a un tiempo de espera de 1 minuto, que el usuario no puede configurar.
- Los comandos de escritura reintentable, confirmación reintentable y cancelación reintentables no son compatibles con Amazon DocumentDB. Si utiliza el shell de mongo heredado (no mongosh), no incluya el comando `retryWrites=false` en ninguna cadena de código. El reintento de las escrituras está desactivado de forma predeterminada. Incluir `retryWrites=false` podría provocar un error en comandos de lectura normales.
- Cada instancia de Amazon DocumentDB tiene un límite superior en el número de transacciones simultáneas abiertas en la instancia a la vez. Para conocer los límites, consulte Límites de instancias.
- Para una transacción determinada, el tamaño del registro de transacciones debe ser inferior a 32 MB.
- Amazon DocumentDB admite `count()` dentro de transacciones, pero no todos los controladores admiten esta capacidad. Una alternativa es utilizar la API `countDocuments()`, que convierte la consulta de recuento en una consulta de agregación en el lado del cliente.
- Las transacciones tienen un límite de ejecución de un minuto y las sesiones tienen un tiempo de espera de 30 minutos. Si se agota el tiempo de espera de una transacción, se cancelará y

cualquier comando posterior que se ejecute dentro de la sesión para la transacción existente generará el siguiente error:

```
WriteCommandError({
"ok" : 0,
"operationTime" : Timestamp(1603491424, 627726),
"code" : 251,
"errmsg" : "Given transaction number 0 does not match any in-progress transactions."
}
```

Supervisión y diagnóstico

Con la compatibilidad con las transacciones en Amazon DocumentDB 4.0, se agregaron métricas de CloudWatch adicionales para ayudarle a monitorear sus transacciones.

Nuevas métricas de CloudWatch

- `DatabaseTransactions`: el número de transacciones abiertas realizadas en un período de un minuto.
- `DatabaseTransactionsAborted`: el número de transacciones canceladas realizadas en un período de un minuto.
- `DatabaseTransactionsMax`: el número máximo de transacciones abiertas realizadas en un período de un minuto.
- `TransactionsAborted`: el número de transacciones canceladas en una instancia en un período de un minuto.
- `TransactionsCommitted`: el número de transacciones confirmadas en una instancia en un período de un minuto.
- `TransactionsOpen`: el número de transacciones abiertas en una instancia en un período de un minuto.
- `TransactionsOpenMax`: el número máximo de transacciones abiertas en una instancia en un período de un minuto.
- `TransactionsStarted`: el número de transacciones canceladas en una instancia en un período de un minuto.

> **Note**
>
> Para obtener más métricas de CloudWatch para Amazon DocumentDB, vaya a Supervisión de Amazon DocumentDB con CloudWatch.

Además, se agregaron nuevos campos a `currentOp` `lsid`, `transactionThreadId`, y un nuevo estado para "`idle transaction`" y las transacciones `serverStatus`: `currentActive`, `currentInactive`, `currentOpen`, `totalAborted`, `totalCommitted` y `totalStarted`.

Nivel de aislamiento de transacciones

Al iniciar una transacción, puede especificar tanto `readConcern` como `writeConcern`, de la forma como se muestra en el siguiente ejemplo:

```
mySession.startTransaction({readConcern: {level: 'snapshot'}, writeConcern:
{w: 'majority'}});
```

Para `readConcern`, Amazon DocumentDB admite el aislamiento de instantáneas de forma predeterminada. Si se especifica una `readConcern` local, disponible o mayoritario, Amazon DocumentDB actualizará el nivel de `readConcern` a instantánea. Amazon DocumentDB no admite el `readConcern` linealizable y, si se especifica una preocupación de lectura de este tipo, se producirá un error.

Para `writeConcern`, Amazon DocumentDB admite la mayoría de forma predeterminada y se logra un quórum de escritura cuando se conservan cuatro copias de los datos en tres zonas de disponibilidad. Si se especifica una `writeConcern` inferior, Amazon DocumentDB la actualizará la `writeConcern` a la mayoría. Además, todas las escrituras de Amazon DocumentDB se registran en un diario y no se puede deshabilitar.

Casos de uso

En esta sección, analizaremos dos casos de uso de las transacciones: varias declaraciones y varias recopilaciones.

Transacciones con varios estados de cuenta

Las transacciones de Amazon DocumentDB son de varios estados, lo que significa que puede escribir una transacción que abarque varios estados con una confirmación o reversión explícita.

Puede agrupar acciones de `insert`, `update`, `delete` y `findAndModify` como una sola operación atómica.

Un caso de uso común para las transacciones con varios estados de cuenta es una transacción de débito-crédito. Por ejemplo: le debe dinero a un amigo de unas prendas de ropa. Por lo tanto, debe cargar (retirar) $500 de su cuenta y acreditar $500 (depósito) en la cuenta de su amigo. Para realizar esa operación, debe realizar las operaciones de débito y crédito en una sola transacción para garantizar la atomicidad. Si lo hace, evitará que se debiten $500 de su cuenta, pero no se acrediten en la cuenta de su amigo. Este es el aspecto que tendría este caso de uso:

```
// *** Transfer $500 from Alice to Bob inside a transaction: Success Scenario***
// Setup bank account for Alice and Bob. Each have $1000 in their account

var databaseName = "bank";
var collectionName = "account";
var amountToTransfer = 500;

var session = db.getMongo().startSession({causalConsistency: false});
var bankDB = session.getDatabase(databaseName);
var accountColl = bankDB[collectionName];
accountColl.drop();

accountColl.insert({name: "Alice", balance: 1000});
accountColl.insert({name: "Bob", balance: 1000});

session.startTransaction();

// deduct $500 from Alice's account
var aliceBalance = accountColl.find({"name": "Alice"}).next().balance;
var newAliceBalance = aliceBalance - amountToTransfer;
accountColl.update({"name": "Alice"},{"$set": {"balance": newAliceBalance}});
var findAliceBalance = accountColl.find({"name": "Alice"}).next().balance;

// add $500 to Bob's account
var bobBalance = accountColl.find({"name": "Bob"}).next().balance;
var newBobBalance = bobBalance + amountToTransfer;
accountColl.update({"name": "Bob"},{"$set": {"balance": newBobBalance}});
var findBobBalance = accountColl.find({"name": "Bob"}).next().balance;

session.commitTransaction();

accountColl.find();
```

```
// *** Transfer $500 from Alice to Bob inside a transaction: Failure Scenario***

// Setup bank account for Alice and Bob. Each have $1000 in their account
var databaseName = "bank";
var collectionName = "account";
var amountToTransfer = 500;

var session = db.getMongo().startSession({causalConsistency: false});
var bankDB = session.getDatabase(databaseName);
var accountColl = bankDB[collectionName];
accountColl.drop();

accountColl.insert({name: "Alice", balance: 1000});
accountColl.insert({name: "Bob", balance: 1000});

session.startTransaction();

// deduct $500 from Alice's account
var aliceBalance = accountColl.find({"name": "Alice"}).next().balance;
var newAliceBalance = aliceBalance - amountToTransfer;
accountColl.update({"name": "Alice"},{"$set": {"balance": newAliceBalance}});
var findAliceBalance = accountColl.find({"name": "Alice"}).next().balance;

session.abortTransaction();
```

Transacciones de varias recopilaciones

Nuestras transacciones también son de cobro múltiple, lo que significa que se pueden utilizar para realizar múltiples operaciones dentro de una sola transacción y en varios cobros. Esto proporciona una visión coherente de los datos y mantiene la integridad de los mismos. Cuando se ejecutan los comandos como un solo <>, las transacciones son ejecuciones de todo o nada, es decir, todas se ejecutarán correctamente o todas fallarán.

A continuación, se muestra un ejemplo de transacciones de varios cobros, en las que se utiliza el mismo escenario y los mismos datos del ejemplo para las transacciones con varios estados de cuenta.

```
// *** Transfer $500 from Alice to Bob inside a transaction: Success Scenario***
```

```
// Setup bank account for Alice and Bob. Each have $1000 in their account
var amountToTransfer = 500;
var collectionName = "account";

var session = db.getMongo().startSession({causalConsistency: false});
var accountCollInBankA = session.getDatabase("bankA")[collectionName];
var accountCollInBankB = session.getDatabase("bankB")[collectionName];

accountCollInBankA.drop();
accountCollInBankB.drop();

accountCollInBankA.insert({name: "Alice", balance: 1000});
accountCollInBankB.insert({name: "Bob", balance: 1000});

session.startTransaction();

// deduct $500 from Alice's account
var aliceBalance = accountCollInBankA.find({"name": "Alice"}).next().balance;
var newAliceBalance = aliceBalance - amountToTransfer;
accountCollInBankA.update({"name": "Alice"},{"$set": {"balance": newAliceBalance}});
var findAliceBalance = accountCollInBankA.find({"name": "Alice"}).next().balance;

// add $500 to Bob's account
var bobBalance = accountCollInBankB.find({"name": "Bob"}).next().balance;
var newBobBalance = bobBalance + amountToTransfer;
accountCollInBankB.update({"name": "Bob"},{"$set": {"balance": newBobBalance}});
var findBobBalance = accountCollInBankB.find({"name": "Bob"}).next().balance;

session.commitTransaction();

accountCollInBankA.find(); // Alice holds $500 in bankA
accountCollInBankB.find(); // Bob holds $1500 in bankB

// *** Transfer $500 from Alice to Bob inside a transaction: Failure Scenario***

// Setup bank account for Alice and Bob. Each have $1000 in their account
var collectionName = "account";
var amountToTransfer = 500;

var session = db.getMongo().startSession({causalConsistency: false});
var accountCollInBankA = session.getDatabase("bankA")[collectionName];
var accountCollInBankB = session.getDatabase("bankB")[collectionName];

accountCollInBankA.drop();
```

```
accountCollInBankB.drop();

accountCollInBankA.insert({name: "Alice", balance: 1000});
accountCollInBankB.insert({name: "Bob", balance: 1000});

session.startTransaction();

// deduct $500 from Alice's account
var aliceBalance = accountCollInBankA.find({"name": "Alice"}).next().balance;
var newAliceBalance = aliceBalance - amountToTransfer;
accountCollInBankA.update({"name": "Alice"},{"$set": {"balance": newAliceBalance}});
var findAliceBalance = accountCollInBankA.find({"name": "Alice"}).next().balance;

// add $500 to Bob's account
var bobBalance = accountCollInBankB.find({"name": "Bob"}).next().balance;
var newBobBalance = bobBalance + amountToTransfer;
accountCollInBankB.update({"name": "Bob"},{"$set": {"balance": newBobBalance}});
var findBobBalance = accountCollInBankB.find({"name": "Bob"}).next().balance;

session.abortTransaction();

accountCollInBankA.find(); // Alice holds $1000 in bankA
accountCollInBankB.find(); // Bob holds $1000 in bankB
```

Ejemplos de API de transacciones para la API de devolución de llamada

La API de devolución de llamada solo está disponible para controladores 4,2 o más.

Javascript

El siguiente código muestra cómo utilizar la API de transacciones de Amazon DocumentDB con Javascript.

```
// *** Transfer $500 from Alice to Bob inside a transaction: Success ***
// Setup bank account for Alice and Bob. Each have $1000 in their account
var databaseName = "bank";
var collectionName = "account";
var amountToTransfer = 500;

var session = db.getMongo().startSession({causalConsistency: false});
var bankDB = session.getDatabase(databaseName);
var accountColl = bankDB[collectionName];
```

```
accountColl.drop();

accountColl.insert({name: "Alice", balance: 1000});
accountColl.insert({name: "Bob", balance: 1000});

session.startTransaction();

// deduct $500 from Alice's account
var aliceBalance = accountColl.find({"name": "Alice"}).next().balance;
assert(aliceBalance >= amountToTransfer);
var newAliceBalance = aliceBalance - amountToTransfer;
accountColl.update({"name": "Alice"},{"$set": {"balance": newAliceBalance}});
var findAliceBalance = accountColl.find({"name": "Alice"}).next().balance;
assert.eq(newAliceBalance, findAliceBalance);

// add $500 to Bob's account
var bobBalance = accountColl.find({"name": "Bob"}).next().balance;
var newBobBalance = bobBalance + amountToTransfer;
accountColl.update({"name": "Bob"},{"$set": {"balance": newBobBalance}});
var findBobBalance = accountColl.find({"name": "Bob"}).next().balance;
assert.eq(newBobBalance, findBobBalance);

session.commitTransaction();

accountColl.find();
```

Node.js

El siguiente código muestra cómo utilizar la API de transacciones de Amazon DocumentDB con Node.js.

```
// Node.js callback API:

const bankDB = await mongoclient.db("bank");
var accountColl = await bankDB.createCollection("account");
var amountToTransfer = 500;

const session = mongoclient.startSession({causalConsistency: false});
await accountColl.drop();

await accountColl.insertOne({name: "Alice", balance: 1000}, { session });
await accountColl.insertOne({name: "Bob", balance: 1000}, { session });
```

```
const transactionOptions = {
    readConcern: { level: 'snapshot' },
    writeConcern: { w: 'majority' }
    };

// deduct $500 from Alice's account
var aliceBalance = await accountColl.findOne({name: "Alice"}, {session});
assert(aliceBalance.balance >= amountToTransfer);
var newAliceBalance = aliceBalance - amountToTransfer;
session.startTransaction(transactionOptions);
await accountColl.updateOne({name: "Alice"}, {$set: {balance: newAliceBalance}},
 {session });
await session.commitTransaction();
aliceBalance = await accountColl.findOne({name: "Alice"}, {session});
assert(newAliceBalance == aliceBalance.balance);

// add $500 to Bob's account
var bobBalance = await accountColl.findOne({name: "Bob"}, {session});
var newBobBalance = bobBalance.balance + amountToTransfer;
session.startTransaction(transactionOptions);
await accountColl.updateOne({name: "Bob"}, {$set: {balance: newBobBalance}},
 {session });
await session.commitTransaction();
bobBalance = await accountColl.findOne({name: "Bob"}, {session});
assert(newBobBalance == bobBalance.balance);
```

C#

El siguiente código muestra cómo utilizar la API de transacciones de Amazon DocumentDB con C#.

```
// C# Callback API

var dbName = "bank";
var collName = "account";
var amountToTransfer = 500;

using (var session = client.StartSession(new ClientSessionOptions{CausalConsistency
 = false}))
{
    var bankDB = client.GetDatabase(dbName);
    var accountColl = bankDB.GetCollection<BsonDocument>(collName);
    bankDB.DropCollection(collName);
```

```
   accountColl.InsertOne(session, new BsonDocument { {"name", "Alice"}, {"balance",
1000 } });
   accountColl.InsertOne(session, new BsonDocument { {"name", "Bob"}, {"balance",
1000 } });

   // start transaction
   var transactionOptions = new TransactionOptions(
           readConcern: ReadConcern.Snapshot,
           writeConcern: WriteConcern.WMajority);
   var result = session.WithTransaction(
       (sess, cancellationtoken) =>
       {
           // deduct $500 from Alice's account
           var aliceBalance = accountColl.Find(sess,
Builders<BsonDocument>.Filter.Eq("name",
"Alice")).FirstOrDefault().GetValue("balance");
           Debug.Assert(aliceBalance >= amountToTransfer);
           var newAliceBalance = aliceBalance.AsInt32 - amountToTransfer;
           accountColl.UpdateOne(sess, Builders<BsonDocument>.Filter.Eq("name",
"Alice"),
                                 Builders<BsonDocument>.Update.Set("balance",
newAliceBalance));
           aliceBalance = accountColl.Find(sess,
Builders<BsonDocument>.Filter.Eq("name",
"Alice")).FirstOrDefault().GetValue("balance");
           Debug.Assert(aliceBalance == newAliceBalance);

           // add $500 from Bob's account
           var bobBalance = accountColl.Find(sess,
Builders<BsonDocument>.Filter.Eq("name",
"Bob")).FirstOrDefault().GetValue("balance");
           var newBobBalance = bobBalance.AsInt32 + amountToTransfer;
           accountColl.UpdateOne(sess, Builders<BsonDocument>.Filter.Eq("name",
"Bob"),
                                 Builders<BsonDocument>.Update.Set("balance",
newBobBalance));
           bobBalance = accountColl.Find(sess,
Builders<BsonDocument>.Filter.Eq("name",
"Bob")).FirstOrDefault().GetValue("balance");
           Debug.Assert(bobBalance == newBobBalance);

           return "Transaction committed";
       }, transactionOptions);
  // check values outside of transaction
```

```
    var aliceNewBalance = accountColl.Find(Builders<BsonDocument>.Filter.Eq("name",
 "Alice")).FirstOrDefault().GetValue("balance");
    var bobNewBalance = accountColl.Find(Builders<BsonDocument>.Filter.Eq("name",
 "Bob")).FirstOrDefault().GetValue("balance");
    Debug.Assert(aliceNewBalance ==  500);
    Debug.Assert(bobNewBalance ==  1500);
}
```

Ruby

El siguiente código muestra cómo utilizar la API de transacciones de Amazon DocumentDB con Ruby.

```
// Ruby Callback API

dbName = "bank"
collName = "account"
amountToTransfer = 500

session = client.start_session(:causal_consistency=> false)
bankDB = Mongo::Database.new(client, dbName)
accountColl = bankDB[collName]
accountColl.drop()

accountColl.insert_one({"name"=>"Alice", "balance"=>1000})
accountColl.insert_one({"name"=>"Bob", "balance"=>1000})

    # start transaction
    session.with_transaction(read_concern: {level: :snapshot}, write_concern:
 {w: :majority}) do
        # deduct $500 from Alice's account
        aliceBalance = accountColl.find({"name"=>"Alice"}, :session=>
 session).first['balance']
        assert aliceBalance >= amountToTransfer
        newAliceBalance = aliceBalance - amountToTransfer
        accountColl.update_one({"name"=>"Alice"}, { "$set" =>
 {"balance"=>newAliceBalance} }, :session=> session)
        aliceBalance = accountColl.find({"name"=>>"Alice"}, :session=>
 session).first['balance']
        assert_equal(newAliceBalance, aliceBalance)

        # add $500 from Bob's account
```

```
        bobBalance = accountColl.find({"name"=>"Bob"}, :session=>
 session).first['balance']
        newBobBalance = bobBalance + amountToTransfer
        accountColl.update_one({"name"=>"Bob"}, { "$set" =>
 {"balance"=>newBobBalance} }, :session=> session)
        bobBalance = accountColl.find({"name"=>"Bob"}, :session=>
 session).first['balance']
        assert_equal(newBobBalance, bobBalance)
    end

   # check results outside of transaction
    aliceBalance = accountColl.find({"name"=>"Alice"}).first['balance']
    bobBalance = accountColl.find({"name"=>"Bob"}).first['balance']
    assert_equal(aliceBalance, 500)
    assert_equal(bobBalance, 1500)

session.end_session
```

Go

El siguiente código muestra cómo utilizar la API de transacciones de Amazon DocumentDB con Go.

```
// Go - Callback API
type Account struct {
    Name string
    Balance  int
}

ctx := context.TODO()

dbName := "bank"
collName := "account"
amountToTransfer := 500

session, err := client.StartSession(options.Session().SetCausalConsistency(false))
assert.NilError(t, err)
defer session.EndSession(ctx)

bankDB := client.Database(dbName)
accountColl := bankDB.Collection(collName)
accountColl.Drop(ctx)
```

```
_, err = accountColl.InsertOne(ctx, bson.M{"name" : "Alice", "balance":1000})
_, err = accountColl.InsertOne(ctx, bson.M{"name" : "Bob", "balance":1000})

transactionOptions := options.Transaction().SetReadConcern(readconcern.Snapshot()).

 SetWriteConcern(writeconcern.New(writeconcern.WMajority()))
_, err = session.WithTransaction(ctx, func(sessionCtx mongo.SessionContext)
 (interface{}, error) {
    var result Account
    // deduct $500 from Alice's account
    err = accountColl.FindOne(sessionCtx, bson.M{"name": "Alice"}).Decode(&result)
    aliceBalance := result.Balance
    newAliceBalance := aliceBalance - amountToTransfer
    _, err = accountColl.UpdateOne(sessionCtx, bson.M{"name": "Alice"},
 bson.M{"$set": bson.M{"balance": newAliceBalance}})
    err = accountColl.FindOne(sessionCtx, bson.M{"name": "Alice"}).Decode(&result)
    aliceBalance = result.Balance
    assert.Equal(t, aliceBalance, newAliceBalance)

    // add $500 to Bob's account
    err = accountColl.FindOne(sessionCtx, bson.M{"name": "Bob"}).Decode(&result)
    bobBalance := result.Balance
    newBobBalance := bobBalance + amountToTransfer
    _, err = accountColl.UpdateOne(sessionCtx, bson.M{"name": "Bob"}, bson.M{"$set":
 bson.M{"balance": newBobBalance}})
    err = accountColl.FindOne(sessionCtx, bson.M{"name": "Bob"}).Decode(&result)
    bobBalance = result.Balance
    assert.Equal(t, bobBalance, newBobBalance)

    if err != nil {
        return nil, err
    }
    return "transaction committed", err
}, transactionOptions)

// check results outside of transaction
var result Account
err = accountColl.FindOne(ctx, bson.M{"name": "Alice"}).Decode(&result)
aliceNewBalance := result.Balance
err = accountColl.FindOne(ctx, bson.M{"name": "Bob"}).Decode(&result)
bobNewBalance := result.Balance
assert.Equal(t, aliceNewBalance, 500)
assert.Equal(t, bobNewBalance, 1500)
```

Java

El siguiente código muestra cómo utilizar la API de transacciones de Amazon DocumentDB con Java.

```
// Java (sync) - Callback API
MongoDatabase bankDB = mongoClient.getDatabase("bank");
MongoCollection accountColl = bankDB.getCollection("account");
accountColl.drop();
int amountToTransfer = 500;

// add sample data
accountColl.insertOne(new Document("name", "Alice").append("balance", 1000));
accountColl.insertOne(new Document("name", "Bob").append("balance", 1000));

TransactionOptions txnOptions = TransactionOptions.builder()
        .readConcern(ReadConcern.SNAPSHOT)
        .writeConcern(WriteConcern.MAJORITY)
        .build();
ClientSessionOptions sessionOptions =
 ClientSessionOptions.builder().causallyConsistent(false).build();
try ( ClientSession clientSession = mongoClient.startSession(sessionOptions) ) {
    clientSession.withTransaction(new TransactionBody<Void>() {
        @Override
        public Void execute() {
            // deduct $500 from Alice's account
            List<Document> documentList = new ArrayList<>();
            accountColl.find(clientSession, new Document("name",
 "Alice")).into(documentList);
            int aliceBalance = (int) documentList.get(0).get("balance");
            int newAliceBalance = aliceBalance - amountToTransfer;

            accountColl.updateOne(clientSession, new Document("name", "Alice"), new
 Document("$set", new Document("balance", newAliceBalance)));

            // check Alice's new balance
            documentList = new ArrayList<>();
            accountColl.find(clientSession, new Document("name",
 "Alice")).into(documentList);
            int updatedBalance = (int) documentList.get(0).get("balance");
            Assert.assertEquals(updatedBalance, newAliceBalance);

            // add $500 to Bob's account
            documentList = new ArrayList<>();
```

```
            accountColl.find(clientSession, new Document("name",
 "Bob")).into(documentList);
            int bobBalance = (int) documentList.get(0).get("balance");
            int newBobBalance = bobBalance + amountToTransfer;

            accountColl.updateOne(clientSession, new Document("name", "Bob"), new
 Document("$set", new Document("balance", newBobBalance)));

            // check Bob's new balance
            documentList = new ArrayList<>();
            accountColl.find(clientSession, new Document("name",
 "Bob")).into(documentList);
            updatedBalance = (int) documentList.get(0).get("balance");
            Assert.assertEquals(updatedBalance, newBobBalance);

            return null;
        }
    }, txnOptions);
}
```

C

El siguiente código muestra cómo utilizar la API de transacciones de Amazon DocumentDB con C.

```
// Sample Code for C with Callback

#include <bson.h>
#include <mongoc.h>
#include <stdio.h>
#include <string.h>
#include <assert.h>

typedef struct {
    int64_t balance;
    bson_t *account;
    bson_t *opts;
    mongoc_collection_t *collection;
} ctx_t;

bool callback_session (mongoc_client_session_t *session, void *ctx, bson_t **reply,
 bson_error_t *error)
{
```

```
    bool r = true;
    ctx_t *data = (ctx_t *) ctx;
    bson_t local_reply;
    bson_t *selector = data->account;
    bson_t *update = BCON_NEW ("$set", "{", "balance", BCON_INT64 (data->balance),
 "}");

    mongoc_collection_update_one (data->collection, selector, update, data->opts,
 &local_reply, error);

    *reply = bson_copy (&local_reply);
    bson_destroy (&local_reply);
    bson_destroy (update);
    return r;
}

void test_callback_money_transfer(mongoc_client_t* client, mongoc_collection_t*
 collection, int amount_to_transfer){

    bson_t reply;
    bool r = true;
    const bson_t *doc;
    bson_iter_t iter;
    ctx_t alice_ctx;
    ctx_t bob_ctx;
    bson_error_t error;

    // find query
    bson_t *alice_query = bson_new ();
    BSON_APPEND_UTF8(alice_query, "name", "Alice");

    bson_t *bob_query = bson_new ();
    BSON_APPEND_UTF8(bob_query, "name", "Bob");

    // create session
    // set causal consistency to false
    mongoc_session_opt_t *session_opts = mongoc_session_opts_new ();
    mongoc_session_opts_set_causal_consistency (session_opts, false);
    // start the session
    mongoc_client_session_t *client_session = mongoc_client_start_session (client,
 session_opts, &error);

    // add session to options
    bson_t *opts = bson_new();
```

```
   mongoc_client_session_append (client_session, opts, &error);

   // deduct 500 from Alice
   // find account balance of Alice
   mongoc_cursor_t *cursor = mongoc_collection_find_with_opts (collection,
alice_query, NULL, NULL);
   mongoc_cursor_next (cursor, &doc);
   bson_iter_init (&iter, doc);
   bson_iter_find (&iter, "balance");
   int64_t alice_balance = (bson_iter_value (&iter))->value.v_int64;
   assert(alice_balance >= amount_to_transfer);
   int64_t new_alice_balance = alice_balance - amount_to_transfer;

   // set variables which will be used by callback function
   alice_ctx.collection = collection;
   alice_ctx.opts = opts;
   alice_ctx.balance = new_alice_balance;
   alice_ctx.account = alice_query;

   // callback
   r = mongoc_client_session_with_transaction (client_session, &callback_session,
NULL, &alice_ctx, &reply, &error);
   assert(r);

   // find account balance of Alice after transaction
   cursor = mongoc_collection_find_with_opts (collection, alice_query, NULL, NULL);
   mongoc_cursor_next (cursor, &doc);
   bson_iter_init (&iter, doc);
   bson_iter_find (&iter, "balance");
   alice_balance = (bson_iter_value (&iter))->value.v_int64;
   assert(alice_balance == new_alice_balance);
   assert(alice_balance == 500);

       // add 500 to bob's balance
   // find account balance of Bob
   cursor = mongoc_collection_find_with_opts (collection, bob_query, NULL, NULL);
   mongoc_cursor_next (cursor, &doc);
   bson_iter_init (&iter, doc);
   bson_iter_find (&iter, "balance");
   int64_t bob_balance = (bson_iter_value (&iter))->value.v_int64;
   int64_t new_bob_balance = bob_balance + amount_to_transfer;

   bob_ctx.collection = collection;
   bob_ctx.opts = opts;
```

```
    bob_ctx.balance = new_bob_balance;
    bob_ctx.account = bob_query;

    // set read & write concern
    mongoc_read_concern_t *read_concern = mongoc_read_concern_new ();
    mongoc_write_concern_t *write_concern = mongoc_write_concern_new ();
    mongoc_transaction_opt_t *txn_opts = mongoc_transaction_opts_new ();

    mongoc_write_concern_set_w(write_concern, MONGOC_WRITE_CONCERN_W_MAJORITY);
    mongoc_read_concern_set_level(read_concern, MONGOC_READ_CONCERN_LEVEL_SNAPSHOT);
    mongoc_transaction_opts_set_write_concern (txn_opts, write_concern);
    mongoc_transaction_opts_set_read_concern (txn_opts, read_concern);

    // callback
    r = mongoc_client_session_with_transaction (client_session, &callback_session,
 txn_opts, &bob_ctx, &reply, &error);
    assert(r);

 // find account balance of Bob after transaction
    cursor = mongoc_collection_find_with_opts (collection, bob_query, NULL, NULL);
    mongoc_cursor_next (cursor, &doc);
    bson_iter_init (&iter, doc);
    bson_iter_find (&iter, "balance");
    bob_balance = (bson_iter_value (&iter))->value.v_int64;
    assert(bob_balance == new_bob_balance);
    assert(bob_balance == 1500);

    // cleanup
    bson_destroy(alice_query);
    bson_destroy(bob_query);
    mongoc_client_session_destroy(client_session);
    bson_destroy(opts);
    mongoc_transaction_opts_destroy(txn_opts);
    mongoc_read_concern_destroy(read_concern);
    mongoc_write_concern_destroy(write_concern);
    mongoc_cursor_destroy(cursor);
    bson_destroy(doc);
}
int main(int argc, char* argv[]) {
    mongoc_init ();
    mongoc_client_t* client = mongoc_client_new (<connection uri>);
    bson_error_t error;

    // connect to bank db
```

```
    mongoc_database_t *database = mongoc_client_get_database (client, "bank");
    // access account collection
    mongoc_collection_t* collection = mongoc_client_get_collection(client, "bank",
 "account");
    // set amount to transfer
    int64_t amount_to_transfer = 500;
    // delete the collection if already existing
    mongoc_collection_drop(collection, &error);

    // open Alice account
    bson_t *alice_account = bson_new ();
    BSON_APPEND_UTF8(alice_account, "name", "Alice");
    BSON_APPEND_INT64(alice_account, "balance", 1000);

    // open Bob account
    bson_t *bob_account = bson_new ();
    BSON_APPEND_UTF8(bob_account, "name", "Bob");
    BSON_APPEND_INT64(bob_account, "balance", 1000);

    bool r = true;

    r = mongoc_collection_insert_one(collection, alice_account, NULL, NULL, &error);
    if (!r) {printf("Error encountered:%s", error.message);}
    r = mongoc_collection_insert_one(collection, bob_account, NULL, NULL, &error);
    if (!r) {printf("Error encountered:%s", error.message);}

    test_callback_money_transfer(client, collection, amount_to_transfer);

}
```

Python

El siguiente código muestra cómo utilizar la API de transacciones de Amazon DocumentDB con Python.

```
// Sample Python code with callback api

import pymongo

def callback(session, balance, query):
    collection.update_one(query, {'$set': {"balance": balance}}, session=session)

client = pymongo.MongoClient(<connection uri>)
```

```
rc_snapshot = pymongo.read_concern.ReadConcern('snapshot')
wc_majority = pymongo.write_concern.WriteConcern('majority')

# To start, drop and create an account collection and insert balances for both Alice
 and Bob
collection = client.get_database("bank").get_collection("account")
collection.drop()
collection.insert_one({"_id": 1, "name": "Alice", "balance": 1000})
collection.insert_one({"_id": 2, "name": "Bob", "balance": 1000})

amount_to_transfer = 500

# deduct 500 from Alice's account
alice_balance = collection.find_one({"name": "Alice"}).get("balance")
assert alice_balance >= amount_to_transfer
new_alice_balance = alice_balance - amount_to_transfer

with client.start_session({'causalConsistency':False}) as session:
    session.with_transaction(lambda s: callback(s, new_alice_balance, {"name":
 "Alice"}), read_concern=rc_snapshot, write_concern=wc_majority)

updated_alice_balance = collection.find_one({"name": "Alice"}).get("balance")
assert updated_alice_balance == new_alice_balance

# add 500 to Bob's account
bob_balance = collection.find_one({"name": "Bob"}).get("balance")
assert bob_balance >= amount_to_transfer
new_bob_balance = bob_balance + amount_to_transfer

with client.start_session({'causalConsistency':False}) as session:
    session.with_transaction(lambda s: callback(s, new_bob_balance, {"name":
 "Bob"}), read_concern=rc_snapshot, write_concern=wc_majority)

updated_bob_balance = collection.find_one({"name": "Bob"}).get("balance")
assert updated_bob_balance == new_bob_balance
```

Ejemplos de API de transacciones para la API de Core

Javascript

El siguiente código muestra cómo utilizar la API de transacciones de Amazon DocumentDB con Javascript.

```
// *** Transfer $500 from Alice to Bob inside a transaction: Success ***
// Setup bank account for Alice and Bob. Each have $1000 in their account
var databaseName = "bank";
var collectionName = "account";
var amountToTransfer = 500;

var session = db.getMongo().startSession({causalConsistency: false});
var bankDB = session.getDatabase(databaseName);
var accountColl = bankDB[collectionName];
accountColl.drop();

accountColl.insert({name: "Alice", balance: 1000});
accountColl.insert({name: "Bob", balance: 1000});

session.startTransaction();

// deduct $500 from Alice's account
var aliceBalance = accountColl.find({"name": "Alice"}).next().balance;
assert(aliceBalance >= amountToTransfer);
var newAliceBalance = aliceBalance - amountToTransfer;
accountColl.update({"name": "Alice"},{"$set": {"balance": newAliceBalance}});
var findAliceBalance = accountColl.find({"name": "Alice"}).next().balance;
assert.eq(newAliceBalance, findAliceBalance);

// add $500 to Bob's account
var bobBalance = accountColl.find({"name": "Bob"}).next().balance;
var newBobBalance = bobBalance + amountToTransfer;
accountColl.update({"name": "Bob"},{"$set": {"balance": newBobBalance}});
var findBobBalance = accountColl.find({"name": "Bob"}).next().balance;
assert.eq(newBobBalance, findBobBalance);

session.commitTransaction();

accountColl.find();
```

C#

El siguiente código muestra cómo utilizar la API de transacciones de Amazon DocumentDB con C#.

```
// C# Core API
```

```
public void TransferMoneyWithRetry(IMongoCollection<bSondocument> accountColl,
 IClientSessionHandle session)
{
    var amountToTransfer = 500;

    // start transaction
   var transactionOptions = new TransactionOptions(
                readConcern: ReadConcern.Snapshot,
                writeConcern: WriteConcern.WMajority);
    session.StartTransaction(transactionOptions);
   try
    {
        // deduct $500 from Alice's account
        var aliceBalance = accountColl.Find(session,
 Builders<bSondocument>.Filter.Eq("name",
 "Alice")).FirstOrDefault().GetValue("balance");
        Debug.Assert(aliceBalance >= amountToTransfer);
        var newAliceBalance = aliceBalance.AsInt32 - amountToTransfer;
        accountColl.UpdateOne(session, Builders<bSondocument>.Filter.Eq("name",
 "Alice"),
                                Builders<bSondocument>.Update.Set("balance",
 newAliceBalance));
        aliceBalance = accountColl.Find(session,
 Builders<bSondocument>.Filter.Eq("name",
 "Alice")).FirstOrDefault().GetValue("balance");
        Debug.Assert(aliceBalance == newAliceBalance);

        // add $500 from Bob's account
        var bobBalance = accountColl.Find(session,
 Builders<bSondocument>.Filter.Eq("name",
 "Bob")).FirstOrDefault().GetValue("balance");
        var newBobBalance = bobBalance.AsInt32 + amountToTransfer;
        accountColl.UpdateOne(session, Builders<bSondocument>.Filter.Eq("name",
 "Bob"),
                                Builders<bSondocument>.Update.Set("balance",
 newBobBalance));
        bobBalance = accountColl.Find(session,
 Builders<bSondocument>.Filter.Eq("name",
 "Bob")).FirstOrDefault().GetValue("balance");
        Debug.Assert(bobBalance == newBobBalance);

    }
    catch (Exception e)
    {
```

```
        session.AbortTransaction();
        throw;
    }

    session.CommitTransaction();
 }

}
public void DoTransactionWithRetry(MongoClient client)
{
    var dbName = "bank";
    var collName = "account";
    using (var session = client.StartSession(new
 ClientSessionOptions{CausalConsistency = false}))
    {
        try
        {
            var bankDB = client.GetDatabase(dbName);
            var accountColl = bankDB.GetCollection<bSondocument>(collName);
            bankDB.DropCollection(collName);
            accountColl.InsertOne(session, new BsonDocument { {"name", "Alice"},
 {"balance", 1000 } });
            accountColl.InsertOne(session, new BsonDocument { {"name", "Bob"},
 {"balance", 1000 } });

            while(true) {
                try
                {
                        TransferMoneyWithRetry(accountColl, session);
                        break;
                }
                catch (MongoException e)
                {
                    if(e.HasErrorLabel("TransientTransactionError"))
                    {
                        continue;
                    }
                    else
                    {
                        throw;
                    }
                }
            }
```

```
            // check values outside of transaction
            var aliceNewBalance =
 accountColl.Find(Builders<bSondocument>.Filter.Eq("name",
 "Alice")).FirstOrDefault().GetValue("balance");
            var bobNewBalance =
 accountColl.Find(Builders<bSondocument>.Filter.Eq("name",
 "Bob")).FirstOrDefault().GetValue("balance");
            Debug.Assert(aliceNewBalance ==  500);
            Debug.Assert(bobNewBalance ==  1500);
        }
        catch (Exception e)
        {
            Console.WriteLine("Error running transaction: " + e.Message);
        }
    }
}
```

Ruby

El siguiente código muestra cómo utilizar la API de transacciones de Amazon DocumentDB con Ruby.

```
# Ruby Core API

def transfer_money_w_retry(session, accountColl)
    amountToTransfer = 500

    session.start_transaction(read_concern: {level: :snapshot}, write_concern:
 {w: :majority})
    # deduct $500 from Alice's account
    aliceBalance = accountColl.find({"name"=>"Alice"}, :session=>
 session).first['balance']
    assert aliceBalance >= amountToTransfer
    newAliceBalance = aliceBalance - amountToTransfer
    accountColl.update_one({"name"=>"Alice"}, { "$set" =>
 {"balance"=>newAliceBalance} }, :session=> session)
    aliceBalance = accountColl.find({"name"=>"Alice"}, :session=>
 session).first['balance']
    assert_equal(newAliceBalance, aliceBalance)

    # add $500 to Bob's account
    bobBalance = accountColl.find({"name"=>"Bob"}, :session=>
 session).first['balance']
```

```
    newBobBalance = bobBalance + amountToTransfer
    accountColl.update_one({"name"=>"Bob"}, { "$set" =>
 {"balance"=>newBobBalance} }, :session=> session)
    bobBalance = accountColl.find({"name"=>"Bob"}, :session=>
 session).first['balance']
    assert_equal(newBobBalance, bobBalance)

    session.commit_transaction

end

def do_txn_w_retry(client)
     dbName = "bank"
    collName = "account"

    session = client.start_session(:causal_consistency=> false)
    bankDB = Mongo::Database.new(client, dbName)
    accountColl = bankDB[collName]
    accountColl.drop()

    accountColl.insert_one({"name"=>"Alice", "balance"=>1000})
    accountColl.insert_one({"name"=>"Bob", "balance"=>1000})

    begin
        transferMoneyWithRetry(session, accountColl)
        puts "transaction committed"
    rescue Mongo::Error => e
        if e.label?('TransientTransactionError')
            retry
        else
            puts "transaction failed"
            raise
        end
    end

    # check results outside of transaction
    aliceBalance = accountColl.find({"name"=>"Alice"}).first['balance']
    bobBalance = accountColl.find({"name"=>"Bob"}).first['balance']
    assert_equal(aliceBalance, 500)
    assert_equal(bobBalance, 1500)

end
```

Go

El siguiente código muestra cómo utilizar la API de transacciones de Amazon DocumentDB con Go.

```
// Go - Core API
type Account struct {
    Name string
    Balance  int
}

func transferMoneyWithRetry(sessionContext mongo.SessionContext, accountColl
 *mongo.Collection, t *testing.T) error {
    amountToTransfer := 500

    transactionOptions :=
 options.Transaction().SetReadConcern(readconcern.Snapshot()).

 SetWriteConcern(writeconcern.New(writeconcern.WMajority()))
    if err := sessionContext.StartTransaction(transactionOptions); err != nil {
        panic(err)
    }

    var result Account
    // deduct $500 from Alice's account
    err := accountColl.FindOne(sessionContext, bson.M{"name":
 "Alice"}).Decode(&result)
    aliceBalance := result.Balance
    newAliceBalance := aliceBalance - amountToTransfer
    _, err = accountColl.UpdateOne(sessionContext, bson.M{"name": "Alice"},
 bson.M{"$set": bson.M{"balance": newAliceBalance}})
    if err != nil {
        sessionContext.AbortTransaction(sessionContext)
    }
    err = accountColl.FindOne(sessionContext, bson.M{"name":
 "Alice"}).Decode(&result)
    aliceBalance = result.Balance
    assert.Equal(t, aliceBalance, newAliceBalance)

    // add $500 to Bob's account
    err = accountColl.FindOne(sessionContext, bson.M{"name": "Bob"}).Decode(&result)
    bobBalance := result.Balance
    newBobBalance := bobBalance + amountToTransfer
```

```
    _, err = accountColl.UpdateOne(sessionContext, bson.M{"name": "Bob"},
 bson.M{"$set": bson.M{"balance": newBobBalance}})
    if err != nil {
        sessionContext.AbortTransaction(sessionContext)
    }
    err = accountColl.FindOne(sessionContext, bson.M{"name": "Bob"}).Decode(&result)
    bobBalance = result.Balance
    assert.Equal(t, bobBalance, newBobBalance)

    err = sessionContext.CommitTransaction(sessionContext)
    return err
}

func doTransactionWithRetry(t *testing.T) {
    ctx := context.TODO()

    dbName := "bank"
    collName := "account"
    bankDB := client.Database(dbName)
    accountColl := bankDB.Collection(collName)

    client.UseSessionWithOptions(ctx, options.Session().SetCausalConsistency(false),
 func(sessionContext mongo.SessionContext) error {
        accountColl.Drop(ctx)
        accountColl.InsertOne(sessionContext, bson.M{"name" : "Alice",
 "balance":1000})
        accountColl.InsertOne(sessionContext, bson.M{"name" : "Bob",
 "balance":1000})
        for {
            err := transferMoneyWithRetry(sessionContext, accountColl, t)
            if err == nil {
                println("transaction committed")
                return nil
            }
            if mongoErr := err.(mongo.CommandError);
 mongoErr.HasErrorLabel("TransientTransactionError") {
                continue
            }
            println("transaction failed")
            return err
        }
    })

    // check results outside of transaction
```

```
    var result Account
    accountColl.FindOne(ctx, bson.M{"name": "Alice"}).Decode(&result)
    aliceBalance := result.Balance
    assert.Equal(t, aliceBalance, 500)
    accountColl.FindOne(ctx, bson.M{"name": "Bob"}).Decode(&result)
    bobBalance := result.Balance
    assert.Equal(t, bobBalance, 1500)
}
```

Java

El siguiente código muestra cómo utilizar la API de transacciones de Amazon DocumentDB con Java.

```
// Java (sync) - Core API

public void transferMoneyWithRetry() {
   // connect to server
    MongoClientURI mongoURI = new MongoClientURI(uri);
    MongoClient mongoClient = new MongoClient(mongoURI);

    MongoDatabase bankDB = mongoClient.getDatabase("bank");
    MongoCollection accountColl = bankDB.getCollection("account");
    accountColl.drop();

   // insert some sample data
    accountColl.insertOne(new Document("name", "Alice").append("balance", 1000));
    accountColl.insertOne(new Document("name", "Bob").append("balance", 1000));

    while (true) {
        try {
            doTransferMoneyWithRetry(accountColl, mongoClient);
            break;
        } catch (MongoException e) {
            if (e.hasErrorLabel(MongoException.TRANSIENT_TRANSACTION_ERROR_LABEL)) {
                continue;
            } else {
                throw e;
            }
        }
    }
}
```

```
public void doTransferMoneyWithRetry(MongoCollection accountColl, MongoClient
 mongoClient) {
    int amountToTransfer = 500;

   TransactionOptions txnOptions = TransactionOptions.builder()
      .readConcern(ReadConcern.SNAPSHOT)
      .writeConcern(WriteConcern.MAJORITY)
      .build();
    ClientSessionOptions sessionOptions =
 ClientSessionOptions.builder().causallyConsistent(false).build();
    try ( ClientSession clientSession = mongoClient.startSession(sessionOptions) ) {
        clientSession.startTransaction(txnOptions);

        // deduct $500 from Alice's account
        List<Document> documentList = new ArrayList<>();
        accountColl.find(clientSession, new Document("name",
 "Alice")).into(documentList);
        int aliceBalance = (int) documentList.get(0).get("balance");
        Assert.assertTrue(aliceBalance >= amountToTransfer);
        int newAliceBalance = aliceBalance - amountToTransfer;
        accountColl.updateOne(clientSession, new Document("name", "Alice"), new
 Document("$set", new Document("balance", newAliceBalance)));

        // check Alice's new balance
        documentList = new ArrayList<>();
        accountColl.find(clientSession, new Document("name",
 "Alice")).into(documentList);
        int updatedBalance = (int) documentList.get(0).get("balance");
        Assert.assertEquals(updatedBalance, newAliceBalance);

        // add $500 to Bob's account
        documentList = new ArrayList<>();
        accountColl.find(clientSession, new Document("name",
 "Bob")).into(documentList);
        int bobBalance = (int) documentList.get(0).get("balance");
        int newBobBalance = bobBalance + amountToTransfer;
        accountColl.updateOne(clientSession, new Document("name", "Bob"), new
 Document("$set", new Document("balance", newBobBalance)));

        // check Bob's new balance
        documentList = new ArrayList<>();
        accountColl.find(clientSession, new Document("name",
 "Bob")).into(documentList);
        updatedBalance = (int) documentList.get(0).get("balance");
```

```
        Assert.assertEquals(updatedBalance, newBobBalance);

        // commit transaction
        clientSession.commitTransaction();
    }
}
// Java (async) -- Core API
public void transferMoneyWithRetry() {
    // connect to the server
    MongoClient mongoClient = MongoClients.create(uri);

    MongoDatabase bankDB = mongoClient.getDatabase("bank");
    MongoCollection accountColl = bankDB.getCollection("account");
    SubscriberLatchWrapper<Void> dropCallback = new SubscriberLatchWrapper<>();
    mongoClient.getDatabase("bank").drop().subscribe(dropCallback);
    dropCallback.await();

    // insert some sample data
    SubscriberLatchWrapper<InsertOneResult> insertionCallback = new
 SubscriberLatchWrapper<>();
    accountColl.insertOne(new Document("name", "Alice").append("balance",
 1000)).subscribe(insertionCallback);
    insertionCallback.await();

    insertionCallback = new SubscriberLatchWrapper<>();
    accountColl.insertOne(new Document("name", "Bob").append("balance",
 1000)).subscribe(insertionCallback);;
    insertionCallback.await();

    while (true) {
        try {
            doTransferMoneyWithRetry(accountColl, mongoClient);
            break;
        } catch (MongoException e) {
            if (e.hasErrorLabel(MongoException.TRANSIENT_TRANSACTION_ERROR_LABEL)) {
                continue;
            } else {
                throw e;
            }
        }
    }
}
```

```
public void doTransferMoneyWithRetry(MongoCollection accountColl, MongoClient
 mongoClient) {
    int amountToTransfer = 500;

    // start the transaction
    TransactionOptions txnOptions = TransactionOptions.builder()
            .readConcern(ReadConcern.SNAPSHOT)
            .writeConcern(WriteConcern.MAJORITY)
            .build();
    ClientSessionOptions sessionOptions =
 ClientSessionOptions.builder().causallyConsistent(false).build();

    SubscriberLatchWrapper<ClientSession> sessionCallback = new
 SubscriberLatchWrapper<>();
    mongoClient.startSession(sessionOptions).subscribe(sessionCallback);
    ClientSession session = sessionCallback.get().get(0);
    session.startTransaction(txnOptions);

    // deduct $500 from Alice's account
    SubscriberLatchWrapper<Document> findCallback = new SubscriberLatchWrapper<>();
    accountColl.find(session, new Document("name",
 "Alice")).first().subscribe(findCallback);
    Document documentFound = findCallback.get().get(0);
    int aliceBalance = (int) documentFound.get("balance");
    int newAliceBalance = aliceBalance - amountToTransfer;

    SubscriberLatchWrapper<UpdateResult> updateCallback = new
 SubscriberLatchWrapper<>();
    accountColl.updateOne(session, new Document("name",
 "Alice"), new Document("$set", new Document("balance",
 newAliceBalance))).subscribe(updateCallback);
    updateCallback.await();

    // check Alice's new balance
    findCallback = new SubscriberLatchWrapper<>();
    accountColl.find(session, new Document("name",
 "Alice")).first().subscribe(findCallback);
    documentFound = findCallback.get().get(0);
    int updatedBalance = (int) documentFound.get("balance");
    Assert.assertEquals(updatedBalance, newAliceBalance);

    // add $500 to Bob's account
    findCallback = new SubscriberLatchWrapper<>();
```

```
    accountColl.find(session, new Document("name",
 "Bob")).first().subscribe(findCallback);
    documentFound = findCallback.get().get(0);
    int bobBalance = (int) documentFound.get("balance");
    int newBobBalance = bobBalance + amountToTransfer;

    updateCallback = new SubscriberLatchWrapper<>();
    accountColl.updateOne(session, new Document("name", "Bob"), new Document("$set",
 new Document("balance", newBobBalance))).subscribe(updateCallback);
    updateCallback.await();

    // check Bob's new balance
    findCallback = new SubscriberLatchWrapper<>();
    accountColl.find(session, new Document("name",
 "Bob")).first().subscribe(findCallback);
    documentFound = findCallback.get().get(0);
    updatedBalance = (int) documentFound.get("balance");
    Assert.assertEquals(updatedBalance, newBobBalance);

    // commit the transaction
    SubscriberLatchWrapper<Void> transactionCallback = new
 SubscriberLatchWrapper<>();
    session.commitTransaction().subscribe(transactionCallback);
    transactionCallback.await();
}

public class SubscriberLatchWrapper<T> implements Subscriber<T> {

    /**
     * A Subscriber that stores the publishers results and provides a latch so can
 block on completion.
     *
     * @param <T> The publishers result type
     */
    private final List<T> received;
    private final List<RuntimeException> errors;
    private final CountDownLatch latch;
    private volatile Subscription subscription;
    private volatile boolean completed;

    /**
     * Construct an instance
     */
    public SubscriberLatchWrapper() {
```

```
        this.received = new ArrayList<>();
        this.errors = new ArrayList<>();
        this.latch = new CountDownLatch(1);
    }

    @Override
    public void onSubscribe(final Subscription s) {
        subscription = s;
        subscription.request(Integer.MAX_VALUE);
    }

    @Override
    public void onNext(final T t) {
        received.add(t);
    }

    @Override
    public void onError(final Throwable t) {
        if (t instanceof RuntimeException) {
            errors.add((RuntimeException) t);
        } else {
            errors.add(new RuntimeException("Unexpected exception", t));
        }
        onComplete();
    }

    @Override
    public void onComplete() {
        completed = true;
        subscription.cancel();
        latch.countDown();
    }

    /**
     * Get received elements
     *
     * @return the list of received elements
     */
    public List<T> getReceived() {
        return received;
    }

    /**
     * Get received elements.
```

```
     *
     * @return the list of receive elements
     */
    public List<T> get() {
        return await().getReceived();
    }

    /**
     * Await completion or error
     *
     * @return this
     */
    public SubscriberLatchWrapper<T> await() {
        subscription.request(Integer.MAX_VALUE);
        try {
            if (!latch.await(300, TimeUnit.SECONDS)) {
                throw new MongoTimeoutException("Publisher onComplete timed out for
 300 seconds");
            }
        } catch (InterruptedException e) {
            throw new MongoInterruptedException("Interrupted waiting for
 observeration", e);
        }
        if (!errors.isEmpty()) {
            throw errors.get(0);
        }
        return this;
    }

    public boolean getCompleted() {
        return this.completed;
    }

    public void close() {
        subscription.cancel();
        received.clear();
    }
}
```

C

El siguiente código muestra cómo utilizar la API de transacciones de Amazon DocumentDB con C.

```
// Sample C code with core session

bool core_session(mongoc_client_session_t *client_session, mongoc_collection_t*
 collection, bson_t *selector, int64_t balance){
    bool r = true;
    bson_error_t error;
    bson_t *opts = bson_new();
    bson_t *update = BCON_NEW ("$set", "{", "balance", BCON_INT64 (balance), "}");

    // set read & write concern
    mongoc_read_concern_t *read_concern = mongoc_read_concern_new ();
    mongoc_write_concern_t *write_concern = mongoc_write_concern_new ();
    mongoc_transaction_opt_t *txn_opts = mongoc_transaction_opts_new ();

    mongoc_write_concern_set_w(write_concern, MONGOC_WRITE_CONCERN_W_MAJORITY);
    mongoc_read_concern_set_level(read_concern, MONGOC_READ_CONCERN_LEVEL_SNAPSHOT);
    mongoc_transaction_opts_set_write_concern (txn_opts, write_concern);
    mongoc_transaction_opts_set_read_concern (txn_opts, read_concern);

    mongoc_client_session_start_transaction (client_session, txn_opts, &error);
    mongoc_client_session_append (client_session, opts, &error);

    r = mongoc_collection_update_one (collection, selector, update, opts, NULL,
 &error);

    mongoc_client_session_commit_transaction (client_session, NULL, &error);
    bson_destroy (opts);
    mongoc_transaction_opts_destroy(txn_opts);
    mongoc_read_concern_destroy(read_concern);
    mongoc_write_concern_destroy(write_concern);
    bson_destroy (update);
    return r;
}

void test_core_money_transfer(mongoc_client_t* client, mongoc_collection_t*
 collection, int amount_to_transfer){

    bson_t reply;
    bool r = true;
    const bson_t *doc;
    bson_iter_t iter;
    bson_error_t error;
```

```
   // find query
   bson_t *alice_query = bson_new ();
   BSON_APPEND_UTF8(alice_query, "name", "Alice");

   bson_t *bob_query = bson_new ();
   BSON_APPEND_UTF8(bob_query, "name", "Bob");

   // create session
   // set causal consistency to false
   mongoc_session_opt_t *session_opts = mongoc_session_opts_new ();
   mongoc_session_opts_set_causal_consistency (session_opts, false);
   // start the session
   mongoc_client_session_t *client_session = mongoc_client_start_session (client,
session_opts, &error);

   // add session to options
   bson_t *opts = bson_new();
   mongoc_client_session_append (client_session, opts, &error);

   // deduct 500 from Alice
   // find account balance of Alice
   mongoc_cursor_t *cursor = mongoc_collection_find_with_opts (collection,
alice_query, NULL, NULL);
   mongoc_cursor_next (cursor, &doc);
   bson_iter_init (&iter, doc);
   bson_iter_find (&iter, "balance");
   int64_t alice_balance = (bson_iter_value (&iter))->value.v_int64;
   assert(alice_balance >= amount_to_transfer);
   int64_t new_alice_balance = alice_balance - amount_to_transfer;

   // core
   r = core_session (client_session, collection, alice_query, new_alice_balance);
   assert(r);

   // find account balance of Alice after transaction
   cursor = mongoc_collection_find_with_opts (collection, alice_query, NULL, NULL);
   mongoc_cursor_next (cursor, &doc);
   bson_iter_init (&iter, doc);
   bson_iter_find (&iter, "balance");
   alice_balance = (bson_iter_value (&iter))->value.v_int64;
   assert(alice_balance == new_alice_balance);
   assert(alice_balance == 500);

   // add 500 to Bob's balance
```

```
    // find account balance of Bob
    cursor = mongoc_collection_find_with_opts (collection, bob_query, NULL, NULL);
    mongoc_cursor_next (cursor, &doc);
    bson_iter_init (&iter, doc);
    bson_iter_find (&iter, "balance");
    int64_t bob_balance = (bson_iter_value (&iter))->value.v_int64;
    int64_t new_bob_balance = bob_balance + amount_to_transfer;

    //core
    r = core_session (client_session, collection, bob_query, new_bob_balance);
    assert(r);

    // find account balance of Bob after transaction
    cursor = mongoc_collection_find_with_opts (collection, bob_query, NULL, NULL);
    mongoc_cursor_next (cursor, &doc);
    bson_iter_init (&iter, doc);
    bson_iter_find (&iter, "balance");
    bob_balance = (bson_iter_value (&iter))->value.v_int64;
    assert(bob_balance == new_bob_balance);
    assert(bob_balance == 1500);

    // cleanup
    bson_destroy(alice_query);
    bson_destroy(bob_query);
    mongoc_client_session_destroy(client_session);
    bson_destroy(opts);
    mongoc_cursor_destroy(cursor);
    bson_destroy(doc);
}

int main(int argc, char* argv[]) {
    mongoc_init ();
    mongoc_client_t* client = mongoc_client_new (<connection uri>);
    bson_error_t error;

    // connect to bank db
    mongoc_database_t *database = mongoc_client_get_database (client, "bank");
    // access account collection
    mongoc_collection_t* collection = mongoc_client_get_collection(client, "bank",
 "account");
    // set amount to transfer
    int64_t amount_to_transfer = 500;
    // delete the collection if already existing
    mongoc_collection_drop(collection, &error);
```

```
    // open Alice account
    bson_t *alice_account = bson_new ();
    BSON_APPEND_UTF8(alice_account, "name", "Alice");
    BSON_APPEND_INT64(alice_account, "balance", 1000);

    // open Bob account
    bson_t *bob_account = bson_new ();
    BSON_APPEND_UTF8(bob_account, "name", "Bob");
    BSON_APPEND_INT64(bob_account, "balance", 1000);

    bool r = true;

    r = mongoc_collection_insert_one(collection, alice_account, NULL, NULL, &error);
    if (!r) {printf("Error encountered:%s", error.message);}
    r = mongoc_collection_insert_one(collection, bob_account, NULL, NULL, &error);
    if (!r) {printf("Error encountered:%s", error.message);}

    test_core_money_transfer(client, collection, amount_to_transfer);

}
```

Scala

El siguiente código muestra cómo utilizar la API de transacciones de Amazon DocumentDB con Scala.

```
// Scala Core API
def transferMoneyWithRetry(sessionObservable: SingleObservable[ClientSession] ,
 database: MongoDatabase ): Unit = {
    val accountColl = database.getCollection("account")
    var amountToTransfer = 500

    var transactionObservable: Observable[ClientSession] =
 sessionObservable.map(clientSession => {
    clientSession.startTransaction()

    // deduct $500 from Alice's account
    var aliceBalance = accountColl.find(clientSession, Document("name" ->
 "Alice")).await().head.getInteger("balance")
    assert(aliceBalance >= amountToTransfer)
    var newAliceBalance = aliceBalance - amountToTransfer
```

```
    accountColl.updateOne(clientSession, Document("name" -> "Alice"),
 Document("$set" -> Document("balance" -> newAliceBalance))).await()
    aliceBalance = accountColl.find(clientSession, Document("name" ->
 "Alice")).await().head.getInteger("balance")
    assert(aliceBalance == newAliceBalance)

    // add $500 to Bob's account
    var bobBalance = accountColl.find(clientSession, Document("name" ->
 "Bob")).await().head.getInteger("balance")
    var newBobBalance = bobBalance + amountToTransfer
    accountColl.updateOne(clientSession, Document("name" -> "Bob"), Document("$set"
 -> Document("balance" -> newBobBalance))).await()
    bobBalance = accountColl.find(clientSession, Document("name" ->
 "Bob")).await().head.getInteger("balance")
    assert(bobBalance == newBobBalance)

    clientSession
    })

    transactionObservable.flatMap(clientSession =>
 clientSession.commitTransaction()).await()
}

def doTransactionWithRetry(): Unit = {
    val client: MongoClient = MongoClientWrapper.getMongoClient()
    val database: MongoDatabase = client.getDatabase("bank")
    val accountColl = database.getCollection("account")
    accountColl.drop().await()

    val sessionOptions =
 ClientSessionOptions.builder().causallyConsistent(false).build()
    var  sessionObservable: SingleObservable[ClientSession] =
 client.startSession(sessionOptions)
    accountColl.insertOne(Document("name" -> "Alice", "balance" -> 1000)).await()
    accountColl.insertOne(Document("name" -> "Bob", "balance" -> 1000)).await()

    var retry = true
    while (retry) {
        try {
        transferMoneyWithRetry(sessionObservable, database)
        println("transaction committed")
        retry = false
        }
        catch {
```

```
        case e: MongoException if
 e.hasErrorLabel(MongoException.TRANSIENT_TRANSACTION_ERROR_LABEL) => {
            println("retrying transaction")
        }
        case other: Throwable => {
            println("transaction failed")
            retry = false
            throw other

        }
        }
    }

    // check results outside of transaction
    assert(accountColl.find(Document("name" ->
 "Alice")).results().head.getInteger("balance") == 500)
    assert(accountColl.find(Document("name" ->
 "Bob")).results().head.getInteger("balance") == 1500)

    accountColl.drop().await()

}
```

Python

El siguiente código muestra cómo utilizar la API de transacciones de Amazon DocumentDB con Python.

```
// Sample Python code with Core api

import pymongo

client = pymongo.MongoClient(<connection_string>)
rc_snapshot = pymongo.read_concern.ReadConcern('snapshot')
wc_majority = pymongo.write_concern.WriteConcern('majority')

# To start, drop and create an account collection and insert balances for both Alice
 and Bob
collection = client.get_database("bank").get_collection("account")
collection.drop()
collection.insert_one({"_id": 1, "name": "Alice", "balance": 1000})
collection.insert_one({"_id": 2, "name": "Bob", "balance": 1000})
```

```
amount_to_transfer = 500

# deduct 500 from Alice's account
alice_balance = collection.find_one({"name": "Alice"}).get("balance")
assert alice_balance >= amount_to_transfer
new_alice_balance = alice_balance - amount_to_transfer

with client.start_session({'causalConsistency':False}) as session:
    session.start_transaction(read_concern=rc_snapshot, write_concern=wc_majority)
    collection.update_one({"name": "Alice"}, {'$set': {"balance":
 new_alice_balance}}, session=session)
    session.commit_transaction()

updated_alice_balance = collection.find_one({"name": "Alice"}).get("balance")
assert updated_alice_balance == new_alice_balance

# add 500 to Bob's account
bob_balance = collection.find_one({"name": "Bob"}).get("balance")
assert bob_balance >= amount_to_transfer
new_bob_balance = bob_balance + amount_to_transfer

with client.start_session({'causalConsistency':False}) as session:
    session.start_transaction(read_concern=rc_snapshot, write_concern=wc_majority)
    collection.update_one({"name": "Bob"}, {'$set': {"balance": new_bob_balance}},
 session=session)
    session.commit_transaction()

updated_bob_balance = collection.find_one({"name": "Bob"}).get("balance")
assert updated_bob_balance == new_bob_balance
```

Comandos admitidos

Comando	Compatible
`abortTransaction`	Sí
`commitTransaction`	Sí
`endSessions`	Sí
`killSession`	Sí

Comando	Compatible
`killAllSession`	Sí
`killAllSessionsByPattern`	No
`refreshSessions`	No
`startSession`	Sí

Capacidades no compatibles

Métodos	Etapas o comandos

`db.collection.aggregate()`	`$collStats`
	`$currentOp`
	`$indexStats`
	`$listSessions`
	`$out`

`db.collection.count()`
`db.collection.countDocuments()`
	`$where`
	`$near`
	`$nearSphere`

`db.collection.insert()`	`insert` no se admite si no se ejecuta en una colección existente. Este método es compatible si se dirige a una colección preexistente.

Sesiones

Las sesiones de MongoDB son un marco que se utiliza para admitir escrituras reintentables, coherencia causal, transacciones y administrar operaciones en bases de datos. Cuando se crea una

sesión, el cliente genera un identificador de sesión lógico (lsid) que se utiliza para etiquetar todas las operaciones de esa sesión al enviar comandos al servidor.

Amazon DocumentDB admite el uso de sesiones para habilitar las transacciones, pero no admite la coherencia causal ni las escrituras reintentables.

Al utilizar transacciones en Amazon DocumentDB, una transacción se iniciará desde una sesión mediante la API `session.startTransaction()` y una sesión admite una sola transacción a la vez. Del mismo modo, las transacciones se completan mediante las API commit (`session.commitTransaction()`) o abort (`session.abortTransaction()`).

Coherencia causal

La coherencia causal garantiza que, en una sola sesión de cliente, el cliente observe la coherencia de lectura tras escritura, las lecturas/escrituras monoatómicas y las escrituras sigan a las lecturas, y estas garantías se aplican a todas las instancias de un clúster, no solo a las principales. Amazon DocumentDB no admite la coherencia causal y la siguiente afirmación generará un error.

```
var mySession = db.getMongo().startSession();
var mySessionObject = mySession.getDatabase('test').getCollection('account');

mySessionObject.updateOne({"_id": 2}, {"$inc": {"balance": 400}});
//Result:{ "acknowledged" : true, "matchedCount" : 1, "modifiedCount" : 1 }

mySessionObject.find()
//Error: error: {
//         "ok" : 0,
//         "code" : 303,
//         "errmsg" : "Feature not supported: 'causal consistency'",
//         "operationTime" : Timestamp(1603461817, 493214)
//}

mySession.endSession()
```

Puede deshabilitar la coherencia causal dentro de una sesión. Tenga en cuenta que si lo hace, podrá utilizar el marco de sesiones, pero no ofrecerá garantías de coherencia causal en las lecturas. Al usar Amazon DocumentDB, las lecturas de la instancia principal serán consistentes de lectura tras escritura y las lecturas de las instancias de réplica serán consistentes eventualmente. Las transacciones son el principal caso de uso para utilizar las sesiones.

```
var mySession = db.getMongo().startSession({causalConsistency: false});
var mySessionObject = mySession.getDatabase('test').getCollection('account');

mySessionObject.updateOne({"_id": 2}, {"$inc": {"balance": 400}});
//Result:{ "acknowledged" : true, "matchedCount" : 1, "modifiedCount" : 1 }

mySessionObject.find()
//{ "_id" : 1, "name" : "Bob", "balance" : 100 }
//{ "_id" : 2, "name" : "Alice", "balance" : 1700 }
```

Reintento de las escrituras

Las escrituras reintentables son una capacidad en la que el cliente intentará volver a intentar las operaciones de escritura una vez cuando se produzcan errores de red o si el cliente no puede encontrar la principal. En Amazon DocumentDB, las escrituras que se pueden volver a intentar no se admiten y deben deshabilitarse. Puede deshabilitarla con el comando (`retryWrites=false`) en la cadena de conexión.

> **Note**
>
> Si utiliza el shell de mongo heredado (no mongosh), no incluya el comando `retryWrites=false` en ninguna cadena de código. El reintento de las escrituras está desactivado de forma predeterminada. Incluir `retryWrites=false` podría provocar un error en comandos de lectura normales.

Errores de la transacción

Cuando se utilizan transacciones, hay situaciones en las que se puede devolver un error que indique que el número de transacción no coincide con ninguna transacción en curso.

El error se puede generar en al menos dos escenarios diferentes:

- Una vez transcurrido el tiempo de espera de la transacción de un minuto.
- Tras el reinicio de la instancia (debido a una aplicación de un parche, una recuperación tras un error, etc.), es posible que se produzca este error incluso en los casos en que la transacción se haya hecho correctamente. Durante el reinicio de una instancia, la base de datos no puede

diferenciar entre una transacción que se completó correctamente y una transacción que se canceló. En otras palabras, el estado de finalización de la transacción es ambiguo.

La mejor forma de solucionar este error es hacer que las actualizaciones transaccionales sean idempotentes, por ejemplo, utilizando el mutador `$set` en lugar de una operación de incremento/decremento. Consulte a continuación:

```
{ "ok" : 0,
"operationTime" : Timestamp(1603938167, 1),
"code" : 251,
"errmsg" : "Given transaction number 1 does not match any in-progress transactions."
}
```

Prácticas recomendadas para Amazon DocumentDB

Conozca las prácticas recomendadas para trabajar con Amazon DocumentDB (compatible con MongoDB). Esta sección se actualiza continuamente a medida que se identifican nuevas prácticas recomendadas.

Temas

- Directrices operativas básicas
- Determinación del tamaño de las instancias
- Uso de índices
- Prácticas recomendadas de seguridad
- Optimización de costos
- Uso de métricas para identificar los problemas de rendimiento
- TTL y cargas de trabajo de series temporales
- Migraciones
- Uso de grupos de parámetros de clúster
- Consultas de canalización de agregación
- batchInsert y batchUpdate

Directrices operativas básicas

A continuación se detallan las directrices operativas básicas que se deben seguir al trabajar con Amazon DocumentDB. El acuerdo de nivel de servicios de Amazon DocumentDB requiere que se sigan estas directrices.

- Implemente un clúster compuesto por dos o más instancias de Amazon DocumentDB en dos zonas de AWS disponibilidad. Para cargas de trabajo de producción, recomendamos implementar un clúster que conste de tres o más instancias de Amazon DocumentDB en tres zonas de disponibilidad.
- Utilice el servicio dentro de los límites de servicio indicados. Para obtener más información, consulte Cuotas y límites de Amazon DocumentDB.
- Monitorice el uso de la memoria, la CPU, las conexiones y el almacenamiento. Para ayudarte a mantener el rendimiento y la disponibilidad del sistema, configura Amazon CloudWatch para

que te notifique cuando cambien los patrones de uso o cuando te acerques a la capacidad de tu implementación.

- Escale las instancias verticalmente cuando se esté acercando a los límites de la capacidad. Las instancias deben aprovisionarse con suficientes recursos informáticos (es decir, RAM, CPU, etc.) para adaptarse a aumentos imprevistos en la demanda de las aplicaciones.
- Configure el periodo de retención de copia de seguridad para ajustarlo a su objetivo de punto de recuperación.
- Pruebe la conmutación por error del clúster para comprender cuánto tiempo tarda el proceso en su caso de uso. Para obtener más información, consulte Conmutación por error a Amazon DocumentDB.
- Conéctese al clúster de Amazon DocumentDB utilizando el punto de conexión del clúster (consulte Puntos de conexión de Amazon DocumentDB) y el modo de conjunto de réplicas (consulte Conexión a Amazon DocumentDB como conjunto de réplicas) para minimizar el impacto de una conmutación por error en la aplicación.
- Elija una configuración de preferencia de lectura de controlador que maximice el escalado de lectura mientras cumple con los requisitos de coherencia de lectura de su aplicación. Las preferencias de lectura `secondaryPreferred` permiten las lecturas de réplica y libera la instancia principal para hacer más trabajo. Para obtener más información, consulte Opciones de preferencia de lectura.
- Diseñe su aplicación para que sea resistente en el caso de que se produzcan errores de la red y de la base de datos. Utilice el mecanismo de errores del controlador para distinguir entre errores temporales y errores persistentes. Reintente los errores temporales mediante un mecanismo de retroceso exponencial cuando sea apropiado. Asegúrese de que la aplicación tenga en cuenta la coherencia de datos al implementar la lógica de reintentos.
- Habilite la protección contra eliminación de clústeres para todos los clústeres de producción o cualquier clúster que tenga datos importantes. Antes de eliminar un clúster de Amazon DocumentDB, tome una instantánea final. Si va a implementar recursos con CloudFormation, habilite la protección de terminación. Para obtener más información, consulte Protección de terminación y protección de eliminación.
- Cuando crea un clúster de Amazon DocumentDB, la `--engine-version` es un parámetro opcional que es el valor predeterminado de la última versión principal del motor. La versión actual del motor principal es la 5.0.0. Cuando se publiquen nuevas versiones principales del motor, la versión del motor predeterminada para `--engine-version` se actualizará para reflejar la última versión principal del motor. Por lo tanto, para las cargas de trabajo de producción, y especialmente

las que dependen de la creación de scripts, la automatización o CloudFormation las plantillas, le recomendamos que especifique explícitamente la versión principal prevista. `--engine-version`

Determinación del tamaño de las instancias

Uno de los aspectos más importantes a la hora de elegir un tamaño de instancia en Amazon DocumentDB es la cantidad de RAM de la memoria caché. Amazon DocumentDB reserva un tercio de la RAM para sus propios servicios, lo que significa que solo dos tercios de la RAM de la instancia están disponibles para la memoria caché. Es una práctica recomendada de rendimiento de Amazon DocumentDB elegir un tipo de instancia con suficiente RAM para que su conjunto de trabajo (es decir, datos e índices) quepa en la memoria. Disponer de instancias del tamaño adecuado ayudará a optimizar el rendimiento general y, potencialmente, a minimizar los I/O costes.

Para determinar si el conjunto de trabajo de su aplicación cabe en la memoria, supervise el `BufferCacheHitRatio` uso de Amazon CloudWatch para cada instancia de un clúster que esté bajo carga.

La `BufferCacheHitRatio` CloudWatch métrica mide el porcentaje de datos e índices servidos desde la caché de memoria de una instancia (en comparación con el volumen de almacenamiento). En términos generales, el valor de `BufferCacheHitRatio` debe ser lo más alto posible, ya que la lectura de datos de la memoria del conjunto de trabajo es más rápida y rentable que la lectura del volumen de almacenamiento. Si bien es deseable mantener `BufferCacheHitRatio` lo más cerca posible del 100 %, el mejor valor alcanzable dependerá de los patrones de acceso y los requisitos de rendimiento de su aplicación. Para mantener el `BufferCacheHitRatio` más alto posible, se recomienda que las instancias del clúster cuenten con suficiente RAM para poder ajustar los índices y el conjunto de datos de trabajo en la memoria.

Si sus índices no caben en la memoria, verá un valor de `BufferCacheHitRatio` inferior. La lectura continua desde el disco implica costos adicionales de E/S y no es mejor que la lectura desde la memoria. Si la proporción de `BufferCacheHitRatio` es inferior a la esperada, escale verticalmente el tamaño de la instancia del clúster para proporcionar más RAM, de forma que los datos del conjunto de trabajo quepan en la memoria. Si escalar la clase de instancia provoca un aumento drástico de `BufferCacheHitRatio`, entonces el conjunto de trabajo de su aplicación no cabe en la memoria. Continúe con el escalado vertical hasta que `BufferCacheHitRatio` ya no aumente drásticamente después de una operación de escalado. Para obtener información acerca del monitoreo de las métricas de una instancia, consulte Métricas de Amazon DocumentDB.

Dependiendo de la carga de trabajo y los requisitos de latencia, puede ser aceptable que la aplicación tenga valores más altos de `BufferCacheHitRatio` durante el uso de estado constante, pero tenga una caída periódica de `BufferCacheHitRatio` a medida que las consultas analíticas que necesitan analizar una colección completa se ejecutan en una instancia. Estas caídas periódicas en `BufferCacheHitRatio` pueden manifestarse como una latencia más alta para consultas posteriores que necesitan volver a llenar los datos del conjunto de trabajo desde el volumen de almacenamiento de nuevo en la caché del búfer. Le recomendamos que pruebe las cargas de trabajo en un entorno de preproducción con una carga de trabajo de producción representativa primero, para comprender las características de rendimiento y **`BufferCacheHitRatio`** antes de implementar la carga de trabajo en producción.

`BufferCacheHitRatio` es una métrica específica de instancia, por lo que las distintas instancias dentro del mismo clúster pueden tener valores de `BufferCacheHitRatio` diferentes, dependiendo de cómo se distribuyen las lecturas entre la instancia principal y la de réplica. Si la carga de trabajo operativa no puede controlar los aumentos periódicos de latencia por volver a llenar la caché del conjunto de trabajo después de ejecutar consultas analíticas, debe intentar aislar la caché del búfer de la carga de trabajo normal de la de las consultas analíticas. Puede lograr un aislamiento completo de `BufferCacheHitRatio` dirigiendo las consultas operativas a la instancia principal y las consultas analíticas solo a las instancias de réplica. También puede lograr un aislamiento parcial dirigiendo consultas analíticas a una instancia de réplica específica, entendiendo que un porcentaje de consultas regulares también se ejecutarán en esa réplica y podrían verse afectadas.

Los valores adecuados de `BufferCacheHitRatio` dependen del caso de uso y los requisitos de la aplicación. No hay un valor máximo o mínimo para esta métrica; solo usted puede decidir si la compensación de un valor de `BufferCacheHitRatio` temporalmente inferior es aceptable desde una perspectiva de costo y rendimiento.

Uso de índices

Creación de índices

Al importar datos en Amazon DocumentDB, debe crear los índices antes de importar grandes conjuntos de datos. Puede utilizar la herramienta de índices de Amazon DocumentDB para extraer índices de una instancia de MongoDB en ejecución o de un directorio `mongodump`, y crear dichos índices en un clúster de Amazon DocumentDB. Para obtener más información acerca de las migraciones, consulte Migración a Amazon DocumentDB.

Selectividad de índice

Se recomienda limitar la creación de índices a campos donde el número de valores duplicados sea inferior al 1 % del número total de documentos de la colección. Por ejemplo, si la colección cuenta con 100 000 documentos, solo cree índices en campos donde el mismo valor se produzca 1000 veces o menos.

Elegir un índice con un alto número de valores únicos (es decir, una alta cardinalidad) garantiza que las operaciones de filtro devuelvan un pequeño número de documentos, con lo que se obtiene un buen rendimiento durante los análisis de índices. Un ejemplo de un índice de alta cardinalidad es un índice único, que garantiza que los predicados de igualdad devuelvan como máximo un documento único. Entre los ejemplos de baja cardinalidad se incluyen un índice sobre un campo booleano y un índice sobre el día de la semana. Debido a su bajo rendimiento, es poco probable que el optimizador de consultas de la base de datos elija índices de cardinalidad baja. Al mismo tiempo, los índices de cardinalidad baja continúan consumiendo recursos como espacio en disco y E/S. Como regla general, debe aplicar los índices a campos donde la frecuencia del valor típica sea un 1 % del tamaño total de la colección o menos.

Además, se recomienda crear índices únicamente en campos que se utilizan comúnmente como filtro y buscar regularmente índices no utilizados. Para obtener más información, consulte ¿Cómo analizo el uso de los índices e identifico los índices no utilizados?.

Impacto de los índices en los datos de escritura

Aunque los índices pueden mejorar el rendimiento de las consultas al evitar la necesidad de examinar todos los documentos de una colección, esta mejora tiene algún inconveniente. Para cada índice de una colección, cada vez que se inserta, actualiza o elimina un documento, la base de datos debe actualizar la colección y escribir los campos en cada uno de los índices de la colección. Por ejemplo, si una colección tiene nueve índices, la base de datos debe realizar diez escrituras antes de validar la operación para el cliente. Por lo tanto, cada índice adicional genera latencia de escritura adicional, E/S y aumento del almacenamiento utilizado en general.

Las instancias del clúster deben tener el tamaño adecuado para mantener toda la memoria del conjunto de trabajo. Esto evita la necesidad de leer continuamente las páginas de índice del volumen de almacenamiento, lo que repercute negativamente en el rendimiento y genera I/O costes más altos. Para obtener más información, consulte Determinación del tamaño de las instancias.

Para obtener un mejor rendimiento, reduzca el número de índices de sus colecciones, agregando solo los índices necesarios para mejorar el rendimiento de las consultas comunes. Aunque las

cargas de trabajo varían, una buena directriz es mantener el número de índices por colección en cinco o menos.

Identificación de índices que faltan

Identificar y eliminar los índices que faltan es una práctica recomendada que aconsejamos realizar de forma periódica. Para obtener más información, consulte ¿Cómo identifico los índices que faltan?.

Identificación de índices no utilizados

Identificar y eliminar índices no utilizados es una práctica recomendada que aconsejamos realizar de forma periódica. Para obtener más información, consulte ¿Cómo analizo el uso de los índices e identifico los índices no utilizados?.

Prácticas recomendadas de seguridad

Como prácticas recomendadas de seguridad, debe usar cuentas AWS Identity and Access Management (IAM) para controlar el acceso a las operaciones de la API de Amazon DocumentDB, especialmente las operaciones que crean, modifican o eliminan los recursos de Amazon DocumentDB. Dichos recursos incluyen clústeres, grupos de seguridad y grupos de parámetros. Debe utilizar también IAM para controlar las acciones administrativas comunes como la restauración de las copias de seguridad de los clústeres. Al crear roles de IAM, utilice el principio de privilegios mínimos.

- Imponga privilegios mínimos con control de acceso basado en roles.
- Asigne una cuenta de IAM individual a cada persona que administre los recursos de Amazon DocumentDB. No utilice el usuario Cuenta de AWS raíz para administrar los recursos de Amazon DocumentDB. Cree un usuario de IAM para todos, incluido usted mismo.
- Conceda a cada usuario de IAM el conjunto mínimo de permisos requerido para realizar sus tareas.
- Use los grupos de IAM para administrar con eficacia los permisos para varios usuarios. Para obtener más información acerca de IAM, consulte la Guía del usuario de IAM. Para obtener información sobre las prácticas recomendadas de IAM, consulte Prácticas recomendadas de IAM.
- Rote con regularidad sus credenciales de IAM.
- Configure AWS Secrets Manager para rotar automáticamente los secretos de Amazon DocumentDB. Para obtener más información, consulte Rotating Your AWS Secrets Manager

Secrets Secrets y Rotating Secrets for Amazon DocumentDB en la Guía del usuario de AWS Secrets Manager.

- Conceda a cada usuario de Amazon DocumentDB el conjunto mínimo de permisos requerido para realizar sus tareas. Para obtener más información, consulte Acceso a la base de datos mediante el control de acceso basado en roles.
- Utilice Transport Layer Security (TLS) para cifrar los datos en tránsito y AWS KMS los datos en reposo.

Optimización de costos

Las siguientes prácticas recomendadas pueden ayudarlo a administrar y minimizar sus costos cuando utilice Amazon DocumentDB. Para obtener información sobre precios, consulte los precios de Amazon DocumentDB (compatible con MongoDB) y Amazon DocumentDB (compatible con MongoDB). FAQs

- Cree alertas de facturación en umbrales del 50 y el 75 % de su factura prevista para el mes. Para obtener más información sobre la creación de alertas de facturación, consulte Creación de una alarma de facturación.
- La arquitectura de Amazon DocumentDB separa el almacenamiento y la computación, por lo que incluso un clúster de una sola instancia es muy duradero. El volumen de almacenamiento del clúster replica los datos de seis formas en tres zonas de disponibilidad, lo que proporciona una durabilidad extremadamente alta con independencia del número de instancias del clúster. Un clúster típico de producción tiene tres o más instancias para proporcionar alta disponibilidad. Sin embargo, puede optimizar los costes mediante un clúster de desarrollo de una única instancia cuando no se requiera alta disponibilidad.
- En las situaciones de desarrollo y pruebas, detenga un clúster cuando ya no sea necesario e inícielo cuando se reanude el desarrollo. Para obtener más información, consulte Detención e inicio de un clúster de bases de datos de Amazon DocumentDB.
- Las secuencias TTL y de cambio generan operaciones de E/S cuando se escriben leen o eliminan datos. Si ha habilitado estas características pero no las está utilizando en la aplicación, su desactivación puede ayudar a reducir los costos.

Uso de métricas para identificar los problemas de rendimiento

Temas

- Visualización de métricas de rendimiento
- Configurar una CloudWatch alarma
- Evaluación de las métricas de rendimiento
- Evaluación del uso de instancias de Amazon DocumentDB con métricas CloudWatch
- Ajuste de consultas

Para identificar los problemas de rendimiento causados por la falta de recursos y otros cuellos de botella frecuentes, puede monitorizar las métricas disponibles para su clúster de base de datos de Amazon DocumentDB.

Visualización de métricas de rendimiento

Monitorice las métricas de desempeño con frecuencia para ver los valores medios, máximos y mínimos de diversos intervalos de tiempo. Esto lo ayuda a identificar cuándo se degrada el rendimiento. También puedes configurar CloudWatch las alarmas de Amazon para determinados umbrales de métricas, de forma que recibas una alerta si se alcanzan.

Para solucionar los problemas de rendimiento, es importante conocer el desempeño de referencia del sistema. Después de configurar un nuevo clúster y ponerlo en marcha con una carga de trabajo típica, capture los valores promedio, máximo y mínimo de todas las métricas de rendimiento en diferentes intervalos (por ejemplo, 1 hora, 24 horas, 1 semana, 2 semanas). Esto permite hacerse una idea de lo que es normal. Ayuda a obtener comparaciones para las horas con picos y valles de funcionamiento. Puede usar esta información para saber cuándo cae el desempeño por debajo de los niveles estándar.

Para ver las métricas de rendimiento, utilice la Consola de administración de AWS tecla o. AWS CLI Para obtener más información, consulte Visualización CloudWatch de datos.

Configurar una CloudWatch alarma

Para configurar una CloudWatch alarma, consulta Uso de Amazon CloudWatch Alarms en la Guía del CloudWatch usuario de Amazon.

Evaluación de las métricas de rendimiento

Una instancia tiene varias categorías diferentes de métricas. La forma de determinar los valores aceptables depende de la métrica.

CPU

- Utilización de la CPU: el porcentaje de la capacidad de procesamiento del equipo que está en uso.

Memoria

- Memoria que se puede liberar: cuánta RAM está disponible en la instancia.
- Uso del espacio de intercambio: cuánto espacio de intercambio usa la instancia en megabytes.

Operaciones de entrada y salida

- IOPS de lectura, IOPS de escritura: número medio de operaciones de lectura o escritura en disco por segundo.
- Latencia de lectura, latencia de escritura: tiempo medio de una operación de lectura o escritura en milisegundos.
- Rendimiento de lectura, rendimiento de escritura: número medio de megabytes leídos o escritos en el disco por segundo.
- Profundidad de la cola del disco: número de operaciones de E/S que esperan para la lectura o escritura en el disco.

Tráfico de red

- Rendimiento de recepción de la red, rendimiento de transmisión de la red: velocidad del tráfico de red de entrada y salida de la instancia de base de datos en megabytes por segundo.

Conexiones a base de datos

- Conexiones a base de datos: número de sesiones cliente que están conectadas a la instancia de base de datos.

En general, los valores aceptables para las métricas de desempeño dependen del aspecto de la referencia y de lo que hace la aplicación. Investigue las variaciones coherentes o de las tendencias con respecto a la referencia.

A continuación, se ofrecen algunas recomendaciones y sugerencias sobre tipos concretos de métricas:

- Consumo elevado de CPU: unos valores elevados de consumo de CPU pueden ser adecuados si se ajustan a los objetivos de su aplicación (de rendimiento o simultaneidad, por ejemplo) y son los esperados. Si el consumo de CPU es sistemáticamente superior al 80 %, valore la posibilidad de escalar las instancias.
- Consumo elevado de RAM: si la métrica `FreeableMemory` se sitúa con frecuencia por debajo del 10% de la memoria total de la instancia, valore la posibilidad de escalar las instancias. Para obtener más información sobre lo que ocurre cuando su instancia de DocumentDB sufre una gran presión de memoria, consulte Amazon DocumentDB Resource Governance.
- Uso de intercambio: esta métrica debe mantenerse en cero o en un valor próximo a cero. Si el uso que hace del intercambio es significativo, valore la posibilidad de escalar las instancias.
- Tráfico de red: para el tráfico de red, hable con el administrador de su sistema para saber cuál es el rendimiento esperado para la red de su dominio y para su conexión a Internet. Investigue el tráfico de red si el rendimiento es por sistema inferior al esperado.
- Conexiones a bases de datos: valore la posibilidad de restringir las conexiones a las bases de datos si ve que hay un alto número de conexiones de usuarios junto con una reducción en el rendimiento y el tiempo de respuesta de la instancia. El mejor número de conexiones de usuarios para su instancia varía en función de la clase de instancia y de la complejidad de las operaciones que se estén llevando a cabo. Si hay problemas con cualquier métrica de desempeño, una de las primeras cosas que debe hacer para mejorar el desempeño es ajustar las consultas más frecuentes y más caras para ver si eso reduce la presión existente en los recursos del sistema.

Si sus consultas están ajustadas y el problema persiste, considere la posibilidad de actualizar la clase de instancia de Amazon DocumentDB a una con más recursos (CPU, RAM, espacio en disco, ancho de banda de red, I/O capacidad) relacionados con el problema que está experimentando.

Evaluación del uso de instancias de Amazon DocumentDB con métricas CloudWatch

Puede usar CloudWatch las métricas para observar el rendimiento de su instancia y descubrir si su clase de instancia proporciona recursos suficientes para sus aplicaciones. Para obtener información sobre los límites de la clase de instancia, vaya a Límites de instancias y busque las especificaciones de la clase de instancia para encontrar el rendimiento de la red.

Si el uso de la instancia está cerca del límite de las clases de instancia, es posible que el rendimiento comience a disminuir. Las CloudWatch métricas pueden confirmar esta situación, por lo que puedes planificar la ampliación manual a una clase de instancias más grande.

Combina los siguientes valores de CloudWatch métricas para saber si te estás acercando al límite de clases de instancias:

- NetworkThroughput—La cantidad de rendimiento de red que reciben y transmiten los clientes para cada instancia del clúster de Amazon DocumentDB. Este valor de rendimiento no incluye el tráfico de red entre las instancias del clúster y el volumen de almacenamiento del clúster.
- StorageNetworkThroughput—La cantidad de rendimiento de red recibida y enviada al volumen de almacenamiento del clúster de Amazon DocumentDB por cada instancia del clúster de Amazon DocumentDB.

Añada el NetworkThroughputal StorageNetworkThroughputpara encontrar el rendimiento de red recibido y enviado al volumen de almacenamiento del clúster de Amazon DocumentDB por cada instancia de su clúster de Amazon DocumentDB. El límite de clases de instancia para su instancia debe ser mayor que la suma de estas dos métricas combinadas.

Puede utilizar las siguientes métricas para revisar detalles adicionales del tráfico de red de las aplicaciones cliente al enviar y recibir:

- NetworkReceiveThroughput—La cantidad de rendimiento de red que recibe de los clientes cada instancia del clúster de Amazon DocumentDB. Este rendimiento no incluye el tráfico de red entre las instancias del clúster y el volumen de almacenamiento del clúster.
- NetworkTransmitThroughput—La cantidad de rendimiento de red que envía a los clientes cada instancia del clúster de Amazon DocumentDB. Este rendimiento no incluye el tráfico de red entre las instancias del clúster y el volumen de almacenamiento del clúster.
- StorageNetworkReceiveThroughput—La cantidad de rendimiento de red recibida del volumen de almacenamiento del clúster de Amazon DocumentDB por cada instancia del clúster.
- StorageNetworkTransmitThroughput—La cantidad de rendimiento de red que cada instancia del clúster envía al volumen de almacenamiento del clúster de Amazon DocumentDB.

Sume todas estas métricas para evaluar cómo está el uso de la red con respecto al límite de las clases de instancias. El límite de las clases de instancias debe ser mayor que la suma de estas métricas combinadas.

Los límites de la red y el uso de la CPU por una instancia son mutuos. Cuando aumenta el rendimiento de la red, también aumenta la utilización de la CPU. La supervisión del uso de la CPU y la red proporciona información sobre cómo y por qué se agotan los recursos.

Para ayudar a minimizar el uso de la red, puede considerar lo siguiente:

- Utilizar una clase de instancia mayor.
- Dividir las solicitudes de escritura en lotes para reducir las transacciones generales.
- Redirigir la carga de trabajo de solo lectura a una instancia de solo lectura.
- Eliminar los índices no utilizados.

Ajuste de consultas

Una de las formas más eficaces de mejorar el rendimiento de clúster es ajustar las consultas más utilizadas y que más recursos consumen para que ejecutarlas resulte más económico.

Puede utilizar el generador de perfiles (consulte Creación de perfiles de operaciones en Amazon DocumentDB) para registrar el tiempo de ejecución y los detalles de las operaciones realizadas en el clúster. El generador de perfiles es útil para monitorizar las operaciones más lentas del clúster para ayudarle a mejorar el rendimiento de las consultas individuales y el rendimiento general del clúster.

También puede utilizar el comando `explain` para descubrir cómo analizar un plan de consulta para una determinada consulta. Utilice esta información para modificar una consulta o una colección subyacente con el fin de mejorar el rendimiento de las consultas (por ejemplo, cómo añadir un índice).

TTL y cargas de trabajo de series temporales

La eliminación de documentos resultante del vencimiento del índice TTL es un proceso muy laborioso. No se garantiza la eliminación de documentos dentro de un periodo específico. Factores como el tamaño de la instancia, la utilización de recursos de la instancia, el tamaño del documento, el rendimiento general, el número de índices y si los índices y el conjunto de trabajo caben en la memoria pueden afectar al momento en el que el proceso TTL elimina los documentos caducados.

Cuando el monitor TTL elimina sus documentos, cada eliminación conlleva I/O costos, lo que aumenta su factura. Si el rendimiento y las tasas de borrado por TTL aumentan, cabe esperar una factura más alta debido al aumento del uso. I/O Sin embargo, si no crea un índice TTL para eliminar documentos, sino que los segmenta en colecciones en función del tiempo y simplemente elimina esas colecciones cuando ya no las necesita, no incurrirá en ningún costo de E/S. Esto puede resultar considerablemente más rentable que utilizar un índice TTL.

Para las cargas de trabajo de series temporales, puede considerar la posibilidad de crear recopilaciones continuas en lugar de un índice TTL, ya que las recopilaciones sucesivas pueden ser una forma mejor de eliminar datos y I/O intensive. If you have large collections (especially collections over 1TB) or TTL deletion I/O costs are a concern, we recommend that you partition documents into collections based on time, and drop collections when the documents are no longer needed. You can create one collection per day or one per week, depending on your data ingest rate. While requirements will vary depending on your application, a good rule of thumb is to have more smaller collections rather than a few large collections. Dropping these collections does not incur I/O reducir costes, además de ser más rápidas y rentables que utilizar un índice TTL.

Migraciones

Como práctica recomendada, recomendamos que al migrar datos a Amazon DocumentDB, primero cree los índices en Amazon DocumentDB antes de migrar los datos. Crear los índices en primer lugar puede reducir el tiempo general y aumentar la velocidad de la migración. Para hacer esto, puede usar la Herramienta de índice de Amazon DocumentDB. Para obtener más información sobre las migraciones, consulte la Guía de migración de Amazon DocumentDB.

También le recomendamos que antes de migrar la base de datos de producción, se recomienda probar completamente la aplicación en Amazon DocumentDB, teniendo en cuenta la funcionalidad, el rendimiento, las operaciones y el costo.

Uso de grupos de parámetros de clúster

Es recomendable que pruebe los cambios de los grupos de parámetros de clúster en un clúster de prueba antes de aplicarlos en los clústeres de producción. Para obtener información acerca del procedimiento para realizar la copia de seguridad del clúster, consulte Copia de seguridad y restauración en Amazon DocumentDB.

Consultas de canalización de agregación

Si crea una consulta de canalización de agregación con varias etapas y evalúa un solo subconjunto de los datos de la consulta, utilice la etapa `$match` como primera etapa o al principio de la canalización. Usar primero `$match` reducirá el número de documentos que las etapas posteriores tendrán que procesar dentro de la consulta de canalización de agregación, mejorando así el rendimiento de su consulta.

`batchInsert` y `batchUpdate`

Cuando se realiza una tasa alta de `batchUpdate` operaciones `batchInsert` simultáneas y la cantidad de `FreeableMemory` (CloudWatch métrica) se reduce a cero en la instancia principal, puede reducir la simultaneidad de la carga de trabajo de inserción o actualización por lotes o, si no se puede reducir la simultaneidad de la carga de trabajo, aumentar el tamaño de la instancia para aumentar la cantidad de`FreeableMemory`.

Diferencias funcionales: Amazon DocumentDB y MongoDB

A continuación se explican las diferencias funcionales entre Amazon DocumentDB (con compatibilidad con MongoDB) y MongoDB.

Temas

- Beneficios funcionales de Amazon DocumentDB
- Diferencias funcionales actualizadas
- Diferencias funcionales con MongoDB

Beneficios funcionales de Amazon DocumentDB

Transacciones implícitas

En Amazon DocumentDB, todas las declaraciones de CRUD (`findAndModify`, `update`, `insert` y `delete`) garantizan la atomicidad y la coherencia, incluso en operaciones que modifican varios documentos. Con el lanzamiento de Amazon DocumentDB 4.0, ahora se admiten transacciones explícitas que proporcionan propiedades ACID para operaciones de varios estados de cuenta y cobros. Para obtener más información sobre el uso de transacciones en Amazon DocumentDB, consulte Transacciones en Amazon DocumentDB.

A continuación se muestran ejemplos de operaciones en Amazon DocumentDB que modifican varios documentos que cumplen los comportamientos de atomicidad y coherencia.

```
db.miles.update(
    { "credit_card": { $eq: true } },
    { $mul: { "flight_miles.$[]": NumberInt(2) } },
    { multi: true }
)
```

```
db.miles.updateMany(
    { "credit_card": { $eq: true } },
    { $mul: { "flight_miles.$[]": NumberInt(2) } }
)
```

```
db.runCommand({
  update: "miles",
  updates: [
    {
      q: { "credit_card": { $eq: true } },
      u: { $mul: { "flight_miles.$[]": NumberInt(2) } },
      multi: true
    }
  ]
})
```

```
db.products.deleteMany({
  "cost": { $gt: 30.00 }
})
```

```
db.runCommand({
  delete: "products",
  deletes: [{ q: { "cost": { $gt: 30.00 } }, limit: 0 }]
})
```

Las operaciones individuales que componen operaciones en bloque tales como `updateMany` y `deleteMany` son atómicas, pero la operación en bloque en su conjunto no es atómica. Por ejemplo, la operación `insertMany` en su conjunto es atómica si las operaciones de inserción individuales se ejecutan correctamente sin errores. Si se detecta algún error en una operación `insertMany`, cada instrucción de inserción individual dentro de la operación `insertMany` se ejecutará como una operación atómica. Si necesita propiedades ACID para operaciones de `insertMany`, `updateMany` y `deleteMany`, se recomienda utilizar una transacción.

Diferencias funcionales actualizadas

Amazon DocumentDB continúa mejorando la compatibilidad con MongoDB al trabajar a partir de las capacidades que nuestros clientes nos piden que creemos. Esta sección contiene las diferencias funcionales que hemos eliminado en Amazon DocumentDB para facilitar las migraciones y la creación de aplicaciones para nuestros clientes.

Temas

- Indexación de matrices
- Índices de varias claves
- Caracteres nulos en cadenas
- Control de acceso con base en roles
- Indexación de $regex
- Proyección para documentos anidados

Indexación de matrices

A partir del 23 de abril de 2020, Amazon DocumentDB admite la capacidad de indexar matrices mayores de 2048 bytes. El límite para un elemento individual en una matriz se mantiene en 2048 bytes, lo que es coherente con MongoDB.

Si crea un nuevo índice, no se necesita ninguna acción para aprovechar la funcionalidad mejorada. Si tiene un índice existente, puede aprovechar la funcionalidad mejorada borrando el índice y después volviéndolo a crear. La versión del índice actual con las capacidades mejoradas es `"v" : 3`.

> **Note**
>
> En el caso de los clústeres de producción, el borrado del índice puede tener un impacto en el rendimiento de la aplicación. Le recomendamos que primero pruebe y proceda con precaución al realizar cambios en un sistema de producción. Además, el tiempo que tardará en volver a crear el índice será una función del tamaño total de los datos de la colección.

Puede consultar la versión de los índices mediante el siguiente comando.

```
db.collection.getIndexes()
```

La salida de esta operación será similar a lo que se indica a continuación. En esta salida, la versión del índice es `"v" : 3`, que es la versión de índice más actual.

```
[
    {
        "v" : 3,
        "key" : {
```

```
        "_id" : 1
        },
        "name" : "_id_",
        "ns" : "test.test"
    }
]
```

Índices de varias claves

A partir del 23 de abril de 2020, Amazon DocumentDB admite la capacidad de crear un índice compuesto por varias claves en la misma matriz.

Si crea un nuevo índice, no se necesita ninguna acción para aprovechar la funcionalidad mejorada. Si tiene un índice existente, puede aprovechar la funcionalidad mejorada borrando el índice y después volviéndolo a crear. La versión del índice actual con las capacidades mejoradas es `"v" : 3`.

> **Note**
>
> En el caso de los clústeres de producción, el borrado del índice puede tener un impacto en el rendimiento de la aplicación. Le recomendamos que primero pruebe y proceda con precaución al realizar cambios en un sistema de producción. Además, el tiempo que tardará en volver a crear el índice será una función del tamaño total de los datos de la colección.

Puede consultar la versión de los índices mediante el siguiente comando.

```
db.collection.getIndexes()
```

La salida de esta operación será similar a lo que se indica a continuación. En esta salida, la versión del índice es `"v" : 3`, que es la versión de índice más actual.

```
[
    {
        "v" : 3,
        "key" : {
            "_id" : 1
        },
        "name" : "_id_",
        "ns" : "test.test"
```

```
    }
]
```

Caracteres nulos en cadenas

A partir del 22 de junio de 2020, Amazon DocumentDB admite ahora caracteres nulos (`'\0'`) en cadenas.

Control de acceso con base en roles

A partir del 26 de marzo de 2020, Amazon DocumentDB admite el control de acceso basado en roles (RBAC) para roles integrados. Para obtener más información, consulte Control de acceso basado en roles.

Indexación de **`$regex`**

A partir del 22 de junio de 2020, Amazon DocumentDB admite la capacidad de los operadores `$regex` de utilizar un índice.

Para utilizar un índice con el operador `$regex`, debe utilizar el comando `hint()`. Al utilizar `hint()`, debe especificar el nombre del campo en el que está aplicando `$regex`. Por ejemplo, si tiene un índice en el campo `product` con el nombre de índice `p_1`, `db.foo.find({product: /^x.*/}).hint({product:1})` utilizará el índice `p_1`, pero `db.foo.find({product: /^x.*/}).hint("p_1")` no utilizará el índice. Puede comprobar si se elige un índice mediante el comando `explain()` o haciendo uso del generador de perfiles para registrar consultas lentas. Por ejemplo, `db.foo.find({product: /^x.*/}).hint("p_1").explain()`.

> **Note**
>
> Solo puede usarse un índice cada vez con el método `hint()`.

El uso de un índice en una consulta `$regex` está optimizado para consultas regex que usan un prefijo y no especifican las opciones `i`, `m` o `o` de regex.

Al utilizar un índice con `$regex`, se recomienda crear un índice en campos altamente selectivos donde el número de valores duplicados sea inferior al 1 % del número total de documentos de la colección. Por ejemplo, si la colección cuenta con 100 000 documentos, solo cree índices en campos donde el mismo valor se produzca 1000 veces o menos.

Proyección para documentos anidados

Existe una diferencia funcional con el operador `$project` entre Amazon DocumentDB y MongoDB en la versión 3.6 que se ha resuelto en Amazon DocumentDB 4.0, pero seguirá sin ser compatible con Amazon DocumentDB 3.6.

Amazon DocumentDB 3.6 solo tiene en cuenta el primer campo de un documento anidado al aplicar una proyección, mientras que MongoDB 3.6 analizará los subdocumentos y aplicará la proyección también a cada subdocumento.

Por ejemplo: si la proyección es `"a.b.c": 1`, se comportará como se esperaba tanto en Amazon DocumentDB como en MongoDB. Sin embargo, si la proyección es `{a:{b:{c:1}}}`, Amazon DocumentDB 3.6 solo aplicará la proyección a `a` y no a `b` o `c`. En Amazon DocumentDB 4.0, la proyección `{a:{b:{c:1}}}` se aplicará a `a`, `b` y `c`.

Diferencias funcionales con MongoDB

Temas

- $vectorSearchoperador
- OpCountersCommand
- Bases de datos de administración y colecciones
- cursormaxTimeMS
- explain()
- Compilaciones de índices
- Búsqueda con una clave vacía en la ruta
- API, operaciones y tipos de datos de MongoDB
- Utilidades de mongodump y mongorestore
- Ordenación de los resultados
- Reintento de las escrituras
- Índices dispersos
- Uso de $elemMatch dentro de una expresión $all
- Dólar($) y punto(.) en los nombres de campos
- $lookup

- $natural y clasificación inversa

`$vectorSearch`operador

Amazon DocumentDB no admite `$vectorSearch` como operador independiente. En su lugar, admitimos `vectorSearch` dentro del operador `$search`. Para obtener más información, consulte Búsqueda vectorial para Amazon DocumentDB.

`OpCountersCommand`

El comportamiento de `OpCountersCommand` de Amazon DocumentDB se desvía de `opcounters.command` de MongoDB de la siguiente manera:

- `opcounters.command` de MongoDB cuenta todos los comandos excepto el de insertar, actualizar y eliminar, mientras que `OpCountersCommand` de Amazon DocumentDB también excluye el comando `find`.
- Amazon DocumentDB tiene en cuenta los comandos internos para `OpCountersCommand`.

Bases de datos de administración y colecciones

Amazon DocumentDB no admite la base de datos de administración o local ni las colecciones `system.*` o `startup_log` de MongoDB, respectivamente.

`cursormaxTimeMS`

En Amazon DocumentDB, `cursor.maxTimeMS` restablece el contador de cada solicitud de `getMore`. Por lo tanto, si se especifica un `maxTimeMS` de 3000 MS, la consulta tarda 2800 MS y cada solicitud de `getMore` posterior tarda 300 MS, por lo que el cursor no agotará el tiempo de espera. El tiempo de espera del cursor solo se agotará cuando una sola operación, ya sea la consulta o una solicitud de `getMore` individual, dure más que el `maxTimeMS` especificado. Además, el barrido que comprueba el tiempo de ejecución del cursor funciona con una granularidad de cinco (5) minutos.

explain()

Amazon DocumentDB emula las API MongoDB 3.6, 4.0 y 5.0 en un motor de base de datos personalizada que utiliza un sistema de almacenamiento distribuido, tolerante a errores y de

recuperación automática. Como resultado, los planes de consulta y la salida de `explain()` pueden diferir entre Amazon DocumentDB y MongoDB. Los clientes que deseen controlar su plan de consulta pueden utilizar el operador `$hint` para aplicar la selección de un índice preferido.

Compilaciones de índices

Amazon DocumentDB solo permite una operación de creación de índice en una colección al mismo tiempo. Ya sea en primer plano o en segundo plano. Si operaciones, tales como `createIndex()` o `dropIndex()`, se producen en la misma colección cuando una operación de creación de índice está actualmente en curso, se producirá un error en la operación que se ha intentado realizar recientemente.

De forma predeterminada, las compilaciones de índices en Amazon DocumentDB y MongoDB versión 4.0 se producen en primer plano. La versión 4.2 y posteriores de MongoDB ignoran la opción de creación de índices en segundo plano si se especifica en createIndexes o sus asistentes de shell `createIndex()` y `createIndexes()`.

Un índice de tiempo de vida (TTL) empieza a marcar los documentos como caducados en cuanto se completa la operación de creación del índice.

Búsqueda con una clave vacía en la ruta

Si busca con una clave que incluye una cadena vacía como parte de la ruta (por ejemplo, `x.`, `x..b`) y el objeto tiene una ruta de clave de cadena vacía (por ejemplo, `{"x" : [ { "" : 10 }, { "b" : 20 } ]}`) dentro de una matriz, Amazon DocumentDB devolverá resultados diferentes a los que arrojaría si usted ejecutara la misma búsqueda en MongoDB.

En MongoDB, la búsqueda de rutas con clave vacía dentro de una matriz funciona tal y como se esperaba cuando la clave de cadena vacía no está al final de la búsqueda de rutas. Sin embargo, cuando la clave de cadena vacía está al final de la búsqueda de rutas, no busca en la matriz.

Sin embargo, en Amazon DocumentDB, solo se lee el primer elemento de la matriz, ya que `getArrayIndexFromKeyString` convierte una cadena vacía en `0`, por lo que se trata a la búsqueda de claves de cadena como a una búsqueda de índice de matriz.

API, operaciones y tipos de datos de MongoDB

Amazon DocumentDB es compatible con las API de MongoDB 3.6, 4.0 y 5.0. Para ver la lista actualizada de funcionalidades admitidas, consulte APIsMongoDB, operaciones y tipos de datos compatibles en Amazon DocumentDB.

Utilidades de **mongodump** y **mongorestore**

Amazon DocumentDB no admite una base de datos de administración y, por lo tanto, no vuelca ni restaura la base de datos de administración cuando se usan las utilidades `mongodump` o `mongorestore`. Al crear una nueva base de datos en Amazon DocumentDB mediante `mongorestore`, debe volver a crear los roles de usuario además de la operación de restauración.

> **Note**
>
> Recomendamos las herramientas de base de datos de MongoDB hasta la versión 100.6.1 inclusive para Amazon DocumentDB. Puede acceder a las descargas de las herramientas de base de datos de MongoDB aquí.

Ordenación de los resultados

Amazon DocumentDB no garantiza la ordenación implícita de los conjuntos de resultados. Para garantizar la ordenación de un conjunto de resultados, especifique explícitamente un criterio de ordenación utilizando `sort()`.

En el siguiente ejemplo, se ordenan los elementos de la colección de inventario en orden descendente en función del campo "stock".

```
db.inventory.find().sort({ stock: -1 })
```

Cuando se utiliza la etapa de agregación de `$sort`, el orden de clasificación no se conserva a menos que la etapa `$sort` sea la última etapa del proceso de agregación. Cuando se utiliza la etapa de agregación de `$sort` en combinación con la etapa de agregación de `$group`, la etapa de agregación de `$sort` solo se aplica a los acumuladores de `$first` y `$last`. En Amazon DocumentDB 4.0, se agregó compatibilidad con `$push` para respetar el orden de clasificación de la etapa de `$sort` anterior.

Reintento de las escrituras

A partir de los controladores compatibles con MongoDB 4.2, el reintento de las escrituras está habilitado de forma predeterminada. Sin embargo, actualmente Amazon DocumentDB no admite el reintento de las escrituras. La diferencia funcional se manifestará en un mensaje de error similar al siguiente.

```
{"ok":0,"errmsg":"Unrecognized field: 'txnNumber'","code":9,"name":"MongoError"}
```

El reintento de las escrituras se puede deshabilitar a través de la cadena de conexión (por ejemplo, `MongoClient("mongodb://my.mongodb.cluster/db?retryWrites=false")`) o el argumento de la palabra clave del constructor MongoClient (por ejemplo, `MongoClient("mongodb://my.mongodb.cluster/db", retryWrites=False)`).

A continuación, se muestra un ejemplo de Python en el que se deshabilita el reintento de las escrituras en la cadena de conexión.

```
client =
 pymongo.MongoClient('mongodb://
<username>:<password>@docdb-2019-03-17-16-49-12.cluster-ccuszbx3pn5e.us-
east-1.docdb.amazonaws.com:27017/?
replicaSet=rs0',w='majority',j=True,retryWrites=False)
```

Índices dispersos

Para utilizar un índice disperso que haya creado en una consulta, debe utilizar la cláusula `$exists` en los campos incluidos en el índice. Si omite `$exists`, Amazon DocumentDB no utilizará el índice disperso.

A continuación se muestra un ejemplo.

```
db.inventory.count({ "stock": { $exists: true }})
```

Para índices dispersos de varias claves, Amazon DocumentDB no admite una restricción de clave única si la búsqueda de un documento da como resultado un conjunto de valores y solo falta un subconjunto de los campos indexados. Por ejemplo, `createIndex({"a.b" : 1 }, { unique : true, sparse :true })` no se admite con la entrada `"a" : [ { "b" : 2 }, { "c" : 1 } ]`, ya que `"a.c"` se almacena en el índice.

Uso de **`$elemMatch`** dentro de una expresión **`$all`**

Actualmente, Amazon DocumentDB no admite el uso del operador `$elemMatch` dentro de una expresión `$all`. Como solución alternativa, puede usar el operador `$and` con `$elemMatch` de la siguiente manera.

Operación original:

```
db.col.find({
  qty: {
    $all: [
      { "$elemMatch": { part: "xyz", qty: { $lt: 11 } } },
      { "$elemMatch": { num: 40, size: "XL" } }
    ]
  }
})
```

Operación actualizada:

```
db.col.find({
  $and: [
    { qty: { "$elemMatch": { part: "xyz", qty: { $lt: 11 } } } },
    { qty: { "$elemMatch": { qty: 40, size: "XL" } } }
  ]
})
```

Dólar($) y punto(.) en los nombres de campos

Amazon DocumentDB no admite la consulta de campos con prefijo dólar($) en $in, $nin y $all en objetos anidados. Por ejemplo, la siguiente consulta no es válida en Amazon DocumentDB.

```
coll.find({"field": {"$all": [{ "$a": 1 }]}})
```

`$lookup`

Amazon DocumentDB admite la posibilidad de llevar a cabo coincidencias de igualdad (por ejemplo, combinación externa izquierda) y también admite subconsultas no correlacionadas, pero no admite subconsultas correlacionadas.

Uso de un índice con `$lookup`

Ahora puede utilizar un índice con el operador de la etapa de `$lookup`. Según su caso de uso, existen varios algoritmos de indexación que puede utilizar para optimizar el rendimiento. En esta sección se explican los diferentes algoritmos de indexación para `$lookup` y se le ayuda a elegir el mejor para su carga de trabajo.

De forma predeterminada, Amazon DocumentDB utilizará el algoritmo hash cuando se utilice `allowDiskUse:false` y se realizará la fusión de clasificación cuando se use `allowDiskUse:true`.

> **Note**
>
> Actualmente, la opción `allowDiskUse` no es compatible con el comando `find`. La opción solo se admite como parte de la agregación. Recomendamos utilizar el marco de agregación con `allowDiskUse:true` para gestionar consultas grandes que puedan superar los límites de memoria.

En algunos casos de uso, puede ser preferible obligar al optimizador de consultas a utilizar un algoritmo diferente. A continuación se muestran los diferentes algoritmos de indexación que puede utilizar el operador de agregación de `$lookup`:

- Bucle anidado: un plan de bucles anidados suele ser beneficioso para una carga de trabajo si la colección externa es inferior a 1 GB y el campo de la colección externa tiene un índice. Si se utiliza el algoritmo de bucle anidado, el plan explicativo mostrará la etapa como `NESTED_LOOP_LOOKUP`.
- Fusión y ordenación: un plan de fusión y ordenación suele ser beneficioso para una carga de trabajo si la colección externa no tiene un índice en el campo utilizado en la búsqueda y el conjunto de datos de trabajo no cabe en la memoria. Si se utiliza el algoritmo de fusión y ordenación, el plan explicativo mostrará la etapa como `SORT_LOOKUP`.
- Hash: un plan de hash suele ser beneficioso para una carga de trabajo si la colección externa ocupa <1 GB y el conjunto de datos de trabajo cabe en la memoria. Si se utiliza el algoritmo de hash, el plan explicativo mostrará la etapa como `HASH_LOOKUP`.

Puede identificar el algoritmo de indexación que se utiliza para el operador de `$lookup` si utiliza `explain` en la consulta. A continuación se muestra un ejemplo:

```
db.localCollection.explain().aggregate(
   [
      {
         $lookup:
            {
               from: "foreignCollection",
               localField: "a",
```

```
               foreignField: "b",
               as: "joined"
            }
      }
   ]
)

output
{
    "queryPlanner" : {
        "plannerVersion" : 1,
        "namespace" : "test.localCollection",
        "winningPlan" : {
            "stage" : "SUBSCAN",
            "inputStage" : {
                "stage" : "SORT_AGGREGATE",
                "inputStage" : {
                    "stage" : "SORT",
                    "inputStage" : {
                        "stage" : "NESTED_LOOP_LOOKUP",
                        "inputStages" : [
                            {
                                "stage" : "COLLSCAN"
                            },
                            {
                                "stage" : "FETCH",
                                "inputStage" : {
                                    "stage" : "COLLSCAN"
                                }
                            }
                        ]
                    }
                }
            }
        }
    },
    "serverInfo" : {
        "host" : "devbox-test",
        "port" : 27317,
        "version" : "3.6.0"
    },
    "ok" : 1
}
```

Como alternativa al uso del método de `explain()`, puede usar el generador de perfiles para revisar el algoritmo que se utiliza al usar el operador de `$lookup`. Para obtener más información acerca del generador de perfiles, consulte Creación de perfiles de operaciones en Amazon DocumentDB.

Uso de una **`planHint`**

Si desea obligar al optimizador de consultas a utilizar un algoritmo de indexación diferente con `$lookup`, puede utilizar un `planHint`. Para ello, utilice el comentario en las opciones de la etapa de agregación para forzar un plan diferente. A continuación, se muestra un ejemplo de la sintaxis del comentario:

```
comment : {
    comment :  "<string>",
    lookupStage : { planHint : "SORT" | "HASH" | "NESTED_LOOP" }
}
```

A continuación, se muestra un ejemplo del uso de `planHint` para obligar al optimizador de consultas a utilizar el algoritmo de indexación HASH:

```
db.foo.aggregate(
   [
      {
         $lookup:
            {
               from: "foo",
               localField: "_id",
               foreignField: "_id",
               as: "joined"
            },
      }
   ]
),
{
   comment : "{ \"lookupStage\" : { \"planHint\": \"HASH\" }}"
```

Para probar qué algoritmo se adapta mejor a su carga de trabajo, puede utilizar el parámetro `executionStats` del método `explain` para medir el tiempo de ejecución de la etapa de `$lookup` y, al mismo tiempo, modificar el algoritmo de indexación (es decir, HASH/SORT/NESTED_LOOP).

El siguiente ejemplo muestra cómo utilizar `executionStats` para medir el tiempo de ejecución de la etapa de `$lookup` mediante el algoritmo de `SORT`.

```
db.foo.explain("executionStats").aggregate(
   [
      {
         $lookup:
            {
               from: "foo",
               localField: "_id",
               foreignField: "_id",
               as: "joined"
            },
      }
   ]
),
{
   comment : "{ \"lookupStage\" : { \"planHint\": \"SORT\" }}"
```

`$natural` y clasificación inversa

Amazon DocumentDB admite `$natural` solamente para escaneos de colecciones reenviados. Los escaneos de colecciones inversos (`{$natural: -1}`) conducirán a un `MongoServerError`.

APIsMongoDB, operaciones y tipos de datos compatibles en Amazon DocumentDB

Amazon DocumentDB (con compatibilidad con MongoDB) es un servicio de base de datos de documentos rápido, completamente administrado, de alta disponibilidad y escala ajustable que admite cargas de trabajo de MongoDB. Amazon DocumentDB es compatible con MongoDB 3.6, 4.0, 5.0 y 8.0. APIs Esta sección muestra la funcionalidad admitida. Para obtener asistencia sobre el uso de APIs MongoDB y los controladores, consulte los foros de la comunidad de MongoDB. Para obtener asistencia con el servicio Amazon DocumentDB, póngase en contacto con el equipo de AWS soporte correspondiente. Para las diferencias funcionales entre Amazon DocumentDB y MongoDB, consulte Diferencias funcionales: Amazon DocumentDB y MongoDB.

Los comandos y operadores de MongoDB que son solo para uso interno o que no se aplican a un servicio completamente administrado no se admiten ni están incluidos en la lista de funcionalidades admitidas.

Hemos agregado más de 50 capacidades adicionales desde el lanzamiento y seguiremos trabajando con versiones anteriores de nuestros clientes para ofrecer las capacidades que necesitan.
Para obtener información sobre los lanzamientos más recientes, consulte Anuncios de Amazon DocumentDB.

Si hay una característica que no es compatible que desea que creemos, háganoslo saber enviando un correo electrónico con su ID de cuenta, las características solicitadas y el caso de uso al equipo de servicio de Amazon DocumentDB.

Temas

- Comandos de la base de datos
- Operadores de consulta y proyección
- Operadores de actualización
- Geospatial (Geoespacial)
- Métodos de cursor
- Operadores de canalización de agregación
- Tipos de datos
- Índices y propiedades de índices

Comandos de la base de datos

Temas

- Comandos administrativos
- Agregación
- Autenticación
- Comandos de diagnóstico
- Operaciones de consulta y escritura
- Comandos para la administración de roles
- Comandos de sesiones
- Administración de usuarios
- Comandos de partición

Comandos administrativos

Comando	3.6	4.0	5.0	8.0	Clúster elástico
Colecciones limitadas	No	No	No	No	No
cloneCollectionAsTapado	No	No	No	No	No
collMod	Parcial	Parcial	Parcial	Parcial	Parcial
CollMod: expireAfterSeconds	Sí	Sí	Sí	Sí	Sí
convertToCapped	No	No	No	No	No
copydb	No	No	No	No	No

Comando	3.6	4.0	5.0	8.0	Clúster elástico
crear	Sí	Sí	Sí	Sí	Sí
createView	No	No	No	Sí	No
createIndexes	Sí	Sí	Sí	Sí	Sí
currentOp	Sí	Sí	Sí	Sí	Sí
drop	Sí	Sí	Sí	Sí	Sí
dropDatabase	Sí	Sí	Sí	Sí	Sí
dropIndexes	Sí	Sí	Sí	Sí	Sí
filemd5	No	No	No	No	No
getAuditConfig	No	Sí	Sí	Sí	No
killCursors	Sí	Sí	Sí	Sí	Sí
killOp	Sí	Sí	Sí	Sí	Sí
listCollections*	Sí	Sí	Sí	Sí	Sí
listDatabases	Sí	Sí	Sí	Sí	Sí
listIndexes	Sí	Sí	Sí	Sí	Sí
reIndex	No	No	Sí	Sí	No
renameCollection	Sí	Sí	Sí	Sí	No

Comando	3.6	4.0	5.0	8.0	Clúster elástico
setAuditConfig	No	Sí	Sí	Sí	No

* No se admite la clave `type` de la opción de filtro.

Agregación

Comando	3.6	4.0	5.0	8.0	Clúster elástico
aggregate	Sí	Sí	Sí	Sí	Sí
count	Sí	Sí	Sí	Sí	Sí
distinct	Sí	Sí	Sí	Sí	Sí
mapReduce	No	No	No	Sí	No

Autenticación

Comando	3.6	4.0	5.0	8.0	Clúster elástico
authenticate	Sí	Sí	Sí	Sí	Sí
logout	Sí	Sí	Sí	Sí	Sí

Comandos de diagnóstico

Comando	3.6	4.0	5.0	8.0	Clúster elástico
buildInfo	Sí	Sí	Sí	Sí	Sí
collStats	Sí	Sí	Sí	Sí	Sí
connPoolStats	No	No	No	No	No
connectionStatus	Sí	Sí	Sí	Sí	Sí
dataSize	Sí	Sí	Sí	Sí	Sí
dbHash	No	No	No	No	No
dbStats	Sí	Sí	Sí	Sí	Sí
explain	Sí	Sí	Sí	Sí	Sí
explain: executionStats	Sí	Sí	Sí	Sí	Sí
Características de	No	No	No	No	No
hostInfo	Sí	Sí	Sí	Sí	Sí
listCommands	Sí	Sí	Sí	Sí	Sí
profiler	Sí	Sí	Sí	Sí	No
serverStatus	Sí	Sí	Sí	Sí	Sí
top	Sí	Sí	Sí	Sí	Sí

Operaciones de consulta y escritura

Comando	3.6	4.0	5.0	8.0	Clúster elástico
Change streams	Sí	Sí	Sí	Sí	No
eliminar	Sí	Sí	Sí	Sí	Sí
find	Sí	Sí	Sí	Sí	Sí
findAndModify	Sí	Sí	Sí	Sí	Sí
getLastError	No	No	No	No	No
getMore	Sí	Sí	Sí	Sí	Sí
getPrevError	No	No	No	No	No
GridFS	Sí	Sí	Sí	Sí	No
inserción	Sí	Sí	Sí	Sí	Sí
parallelCollectionScan	No	No	No	No	No
resetError	No	No	No	No	No
actualización	Sí	Sí	Sí	Sí	Sí
ReplaceOne	Sí	Sí	Sí	Sí	Sí

Comandos para la administración de roles

C	3	4	5	8	C e
c e	Sí	Sí	Sí	Sí	No
c le ta	Sí	Sí	Sí	Sí	No
c	Sí	Sí	Sí	Sí	No
g s	Sí	Sí	Sí	Sí	No
r e	Sí	Sí	Sí	Sí	No
r v c	Sí	Sí	Sí	Sí	No
r	Sí	Sí	Sí	Sí	No
u e	Sí	Sí	Sí	Sí	No

Comandos de sesiones

Comando	3.6	4.0	5.0	8.0	Clúster elástico
Abortar transacción	No	Sí	Sí	Sí	No

Comando	3.6	4.0	5.0	8.0	Clúster elástico
commitTransaction	No	Sí	Sí	Sí	No
Finalizar sesiones	No	No	No	No	No
killAllSessions	No	Sí	Sí	Sí	No
killAllSessionsByPattern	No	No	No	No	No
Mata a Sessions	No	Sí	Sí	Sí	No
Actualizar sesiones	No	No	No	No	No
StartSession	No	Sí	Sí	Sí	No

Administración de usuarios

Comando	3.6	4.0	5.0	8.0	Clúster elástico
createUser	Sí	Sí	Sí	Sí	Sí
dropAllUsersFromDatabase	Sí	Sí	Sí	Sí	Sí
dropUser	Sí	Sí	Sí	Sí	Sí

Comando	3.6	4.0	5.0	8.0	Clúster elástico
grantRolesToUser	Sí	Sí	Sí	Sí	Sí
revokeRolesFromUser	Sí	Sí	Sí	Sí	Sí
updateUser	Sí	Sí	Sí	Sí	Sí
usersInfo	Sí	Sí	Sí	Sí	Sí

Comandos de partición

Comando	Clúster elástico
abortReshardCollection	No
Añadir partición	No
addShardToZona	No
balancerCollectionStatus	No
Balancer Start	No
Estado del equilibrador	No
BalancerStop	No
checkShardingIndex	No
clearJumboFlag	No
cleanupOrphaned	No
cleanupReshardCollection	No
commitReshardCollection	No

Comando	Clúster elástico
Habilitar Sharding	Sí
flushRouterConfig	No
getShardMap	No
getShardVersion	No
isdbgrid	No
ListShards	No
Clave mediana	No
Mueva Chunk	No
Mueva el modo principal	No
MergeChunks	No
refineCollectionShardClave	No
Elimina Hard	No
removeShardFromZona	No
Colección ReShard	No
setAllowMigrations	No
setShardVersion	No
Colección Shard	Sí
Estado de partición	No
dividir	No
Vector dividido	No

Comando	Clúster elástico
UnsetSharding	No
updateZoneKeyAlcance	No

Operadores de consulta y proyección

Temas

- Operadores de matrices
- Operadores Bitwise
- Operador de comentarios
- Operadores de comparación
- Operadores de elementos
- Operadores de consulta de evaluación
- Logical operators (Operadores lógicos)
- Operadores de proyección

Operadores de matrices

Comando	3.6	4.0	5.0	8.0	Clúster elástico
$all	Sí	Sí	Sí	Sí	Sí
$elemMatch	Sí	Sí	Sí	Sí	Sí
$size	Sí	Sí	Sí	Sí	Sí

Operadores Bitwise

Comando	3.6	4.0	5.0	8.0	Clúster elástico
$bitsAllSet	Sí	Sí	Sí	Sí	Sí
$bitsAnySet	Sí	Sí	Sí	Sí	Sí
$bitsAllClear	Sí	Sí	Sí	Sí	Sí
$bitsAnyClear	Sí	Sí	Sí	Sí	Sí

Operador de comentarios

Comando	3.6	4.0	5.0	8.0	Clúster elástico
$comment	Sí	Sí	Sí	Sí	Sí

Operadores de comparación

Comando	3.6	4.0	5.0	8.0	Clúster elástico
$eq	Sí	Sí	Sí	Sí	Sí
$gt	Sí	Sí	Sí	Sí	Sí
$gte	Sí	Sí	Sí	Sí	Sí
$in	Sí	Sí	Sí	Sí	Sí
$lt	Sí	Sí	Sí	Sí	Sí
$lte	Sí	Sí	Sí	Sí	Sí

Comando	3.6	4.0	5.0	8.0	Clúster elástico
$ne	Sí	Sí	Sí	Sí	Sí
$nin	Sí	Sí	Sí	Sí	Sí

Operadores de elementos

Comando	3.6	4.0	5.0	8.0	Clúster elástico
$exists	Sí	Sí	Sí	Sí	Sí
$type	Sí	Sí	Sí	Sí	Sí

Operadores de consulta de evaluación

Comando	3.6	4.0	5.0	8.0	Clúster elástico
$expr	No	Sí	Sí	Sí	No
$jsonSchema	No	Sí	Sí	Sí	No
$mod	Sí	Sí	Sí	Sí	Sí
$regex	Sí	Sí	Sí	Sí	Sí
$text	No	No	Sí	Sí	No
$where	No	No	No	No	No

Logical operators (Operadores lógicos)

Comando	3.6	4.0	5.0	8.0	Clúster elástico
$and	Sí	Sí	Sí	Sí	Sí
$nor	Sí	Sí	Sí	Sí	Sí
$not	Sí	Sí	Sí	Sí	Sí
$or	Sí	Sí	Sí	Sí	Sí

Operadores de proyección

Comando	3.6	4.0	5.0	8.0	Clúster elástico
$	Sí	Sí	Sí	Sí	Sí
$elemMatch	Sí	Sí	Sí	Sí	Sí
$meta	No	No	Sí	Sí	No
$slice	Sí	Sí	Sí	Sí	Sí

Operadores de actualización

Temas

- Operadores de matrices
- Operadores Bitwise
- Operadores de campo
- Modificadores de actualización

Operadores de matrices

Comando	3.6	4.0	5.0	8.0	Clúster elástico
$	Sí	Sí	Sí	Sí	Sí
$[]	Sí	Sí	Sí	Sí	Sí
$[<identifier>]	Sí	Sí	Sí	Sí	Sí
$addToSet	Sí	Sí	Sí	Sí	Sí
$pop	Sí	Sí	Sí	Sí	Sí
$pullAll	Sí	Sí	Sí	Sí	Sí
$pull	Sí	Sí	Sí	Sí	Sí
$push	Sí	Sí	Sí	Sí	Sí

Operadores Bitwise

Comando	3.6	4.0	5.0	8.0	Clúster elástico
$bit	Sí	Sí	Sí	Sí	Sí

Operadores de campo

Operador	3.6	4.0	5.0	8.0	Clúster elástico
$currentDate	Sí	Sí	Sí	Sí	Sí
$inc	Sí	Sí	Sí	Sí	Sí

Operador	3.6	4.0	5.0	8.0	Clúster elástico
$max	Sí	Sí	Sí	Sí	Sí
$min	Sí	Sí	Sí	Sí	Sí
$mul	Sí	Sí	Sí	Sí	Sí
$rename	Sí	Sí	Sí	Sí	Sí
$set	Sí	Sí	Sí	Sí	Sí
$setOnInsert	Sí	Sí	Sí	Sí	Sí
$unset	Sí	Sí	Sí	Sí	Sí

Modificadores de actualización

Operador	3.6	4.0	5.0	8.0	Clúster elástico
$each	Sí	Sí	Sí	Sí	Sí
$position	Sí	Sí	Sí	Sí	Sí
$slice	Sí	Sí	Sí	Sí	Sí
$sort	Sí	Sí	Sí	Sí	Sí

Geospatial (Geoespacial)

Especificadores de geometría

Selectores de consultas	3.6	4.0	5.0	8.0	Clúster elástico
$box	No	No	No	No	No
$center	No	No	No	No	No
$centerSphere	No	No	No	No	No
$geometry	Sí	Sí	Sí	Sí	Sí
$maxDistance	Sí	Sí	Sí	Sí	Sí
$minDistance	Sí	Sí	Sí	Sí	Sí
$nearSphere	Sí	Sí	Sí	Sí	Sí
$polygon	No	No	No	No	No
$uniqueDocs	No	No	No	No	No

Selectores de consultas

Comando	3.6	4.0	5.0	8.0	Clúster elástico
$geoIntersects	Sí	Sí	Sí	Sí	Sí
$geoWithin	Sí	Sí	Sí	Sí	Sí
$near	Sí	Sí	Sí	Sí	Sí

Comando	3.6	4.0	5.0	8.0	Clúster elástico
$nearSphere	Sí	Sí	Sí	Sí	Sí
$polygon	No	No	No	No	No
$uniqueDocs	No	No	No	No	No

Métodos de cursor

Comando	3.6	4.0	5.0	8.0	Clúster elástico
cursor.batchSize()	Sí	Sí	Sí	Sí	Sí
cursor.close()	Sí	Sí	Sí	Sí	Sí
cursor.collation()	No	No	No	Sí	No
cursor.comment()	Sí	Sí	Sí	Sí	Sí
cursor.count()	Sí	Sí	Sí	Sí	Sí
cursor.explain()	Sí	Sí	Sí	Sí	No
cursor.forEach()	Sí	Sí	Sí	Sí	Sí
cursor.hasNext()	Sí	Sí	Sí	Sí	Sí
cursor.hint()	Sí	Sí	Sí	Sí	Sí*

Comando	3.6	4.0	5.0	8.0	Clúster elástico
cursor.isClosed()	Sí	Sí	Sí	Sí	Sí
cursor.isExhausted()	Sí	Sí	Sí	Sí	No
cursor.itcount()	Sí	Sí	Sí	Sí	No
cursor.limit()	Sí	Sí	Sí	Sí	No
cursor.map()	Sí	Sí	Sí	Sí	No
cursor.max()	No	No	No	No	No
cursor.maxScan()	Sí	Sí	Sí	Sí	No
cursor.maxTimeMS()	Sí	Sí	Sí	Sí	No
cursor.min()	No	No	No	No	No
cursor.next()	Sí	Sí	Sí	Sí	Sí
cursor.noCursorTimeout()	No	No	No	No	No
cursor.objsLeftInBatch ()	Sí	Sí	Sí	Sí	No
cursor.pretty()	Sí	Sí	Sí	Sí	No

Comando	3.6	4.0	5.0	8.0	Clúster elástico
cursor.readConcern()	Sí	Sí	Sí	Sí	No
cursor.readPref()	Sí	Sí	Sí	Sí	No
cursor.returnKey()	No	No	No	No	No
cursor.showRecordId()	No	No	No	No	No
cursor.size()	Sí	Sí	Sí	Sí	No
cursor.skip()	Sí	Sí	Sí	Sí	No
cursor.sort()	Sí	Sí	Sí	Sí	No
cursor.tailable()	No	No	No	No	No
cursor.toArray()	Sí	Sí	Sí	Sí	No

* El índice `hint` es compatible con las expresiones de índice. Por ejemplo, `db.foo.find().hint({x:1})`.

Operadores de canalización de agregación

Temas

- Expresiones de acumulación
- Operadores aritméticos
- Operadores de matrices

- Operadores booleanos
- Operadores de comparación
- Operadores de expresiones condicionales
- Operador de tipos de datos
- Operador de tamaño de datos
- Operadores de fechas
- Operador literal
- Operador de combinación
- Operador natural
- Operadores de establecimiento
- Operadores de etapa
- Operadores de cadena
- Variables del sistema
- Operador de búsqueda de texto
- Operadores de conversión de tipos
- Operadores de variables
- Operadores misceláneos

Expresiones de acumulación

Expression	3.6	4.0	5.0	8.0	Clúster elástico
$ acumulador	-	-	No	No	No
$addToSet	Sí	Sí	Sí	Sí	Sí
$avg	Sí	Sí	Sí	Sí	Sí
$count	-	-	No	No	No
$covarianCePop	No	No	No	No	No

Expression	3.6	4.0	5.0	8.0	Clúster elástico
$covarianceSamp	No	No	No	No	No
$denseRank	No	No	No	No	No
$derivative	No	No	No	No	No
$documentNumber	No	No	No	No	No
$expMovingAvg	No	No	No	No	No
$first	Sí	Sí	Sí	Sí	Sí
$integral	No	No	No	No	No
$last	Sí	Sí	Sí	Sí	Sí
$max	Sí	Sí	Sí	Sí	Sí
$min	Sí	Sí	Sí	Sí	Sí
$push	Sí	Sí	Sí	Sí	Sí
$rank	No	No	No	No	No
$shift	No	No	No	No	No
$stdDevPop	No	No	No	No	No
$stdDevSamp	No	No	No	No	No
$sum	Sí	Sí	Sí	Sí	Sí

Operadores aritméticos

Comando	3.6	4.0	5.0	8.0	Clúster elástico
$abs	Sí	Sí	Sí	Sí	Sí
$add	Sí	Sí	Sí	Sí	Sí
$ceil	No	Sí	Sí	Sí	Sí
$divide	Sí	Sí	Sí	Sí	Sí
$exp	No	Sí	Sí	Sí	Sí
$floor	No	Sí	Sí	Sí	Sí
$ln	No	Sí	Sí	Sí	Sí
$log	No	Sí	Sí	Sí	Sí
$log10	No	Sí	Sí	Sí	Sí
$mod	Sí	Sí	Sí	Sí	Sí
$multiply	Sí	Sí	Sí	Sí	Sí
$pow	No	No	No	Sí	No
$round	-	-	No	No	No
$sqrt	No	Sí	Sí	Sí	Sí
$subtract	Sí	Sí	Sí	Sí	Sí
$trunc	No	No	No	No	No

Operadores de matrices

Comando	3.6	4.0	5.0	8.0	Clúster elástico
$arrayElemAt	Sí	Sí	Sí	Sí	Sí
$arrayToObject	Sí	Sí	Sí	Sí	Sí
$concatArrays	Sí	Sí	Sí	Sí	Sí
$filter	Sí	Sí	Sí	Sí	Sí
$first	-	-	Sí	Sí	No
$in	Sí	Sí	Sí	Sí	Sí
$indexOfArray	Sí	Sí	Sí	Sí	Sí
$isArray	Sí	Sí	Sí	Sí	Sí
$last	-	-	Sí	Sí	No
$objectToArray	Sí	Sí	Sí	Sí	Sí
$range	Sí	Sí	Sí	Sí	Sí
$reverseArray	Sí	Sí	Sí	Sí	Sí
$reduce	Sí	Sí	Sí	Sí	Sí
$size	Sí	Sí	Sí	Sí	Sí
$slice	Sí	Sí	Sí	Sí	Sí
$zip	Sí	Sí	Sí	Sí	Sí

Operadores booleanos

Comando	3.6	4.0	5.0	8.0	Clúster elástico
$and	Sí	Sí	Sí	Sí	Sí
$not	Sí	Sí	Sí	Sí	Sí
$or	Sí	Sí	Sí	Sí	Sí

Operadores de comparación

Comando	3.6	4.0	5.0	8.0	Clúster elástico
$cmp	Sí	Sí	Sí	Sí	Sí
$eq	Sí	Sí	Sí	Sí	Sí
$gt	Sí	Sí	Sí	Sí	Sí
$gte	Sí	Sí	Sí	Sí	Sí
$lt	Sí	Sí	Sí	Sí	Sí
$lte	Sí	Sí	Sí	Sí	Sí
$ne	Sí	Sí	Sí	Sí	Sí

Operadores de expresiones condicionales

Comando	3.6	4.0	5.0	8.0	Clúster elástico
$cond	Sí	Sí	Sí	Sí	Sí

Comando	3.6	4.0	5.0	8.0	Clúster elástico
$ifNull	Sí	Sí	Sí	Sí	Sí
$switch	No	Sí	Sí	Sí	No

Operador de tipos de datos

Comando	3.6	4.0	5.0	8.0	Clúster elástico
$type	Sí	Sí	Sí	Sí	Sí

Operador de tamaño de datos

Comando	3.6	4.0	5.0	8.0	Clúster elástico
$binarySize	-	-	No	No	No
$bsonSize	-	-	No	No	No

Operadores de fechas

Comando	3.6	4.0	5.0	8.0	Clúster elástico
$dateAdd	No	No	Sí	Sí	Sí
$dateDiff	-	-	Sí	Sí	No
$dateFromParts	No	No	No	No	No

Comando	3.6	4.0	5.0	8.0	Clúster elástico
$dateFromString	Sí	Sí	Sí	Sí	Sí
$dateSubtract	No	No	Sí	Sí	Sí
$dateToParts	No	No	No	No	No
$dateToString	Sí	Sí	Sí	Sí	Sí
$dateTrunc	-	-	No	Sí	No
$dayOfMonth	Sí	Sí	Sí	Sí	Sí
$dayOfWeek	Sí	Sí	Sí	Sí	Sí
$dayOfYear	Sí	Sí	Sí	Sí	Sí
$hour	Sí	Sí	Sí	Sí	Sí
$ isoDayOf Semana	Sí	Sí	Sí	Sí	Sí
$isoWeek	Sí	Sí	Sí	Sí	Sí
$isoWeekYear	Sí	Sí	Sí	Sí	Sí
$millisecond	Sí	Sí	Sí	Sí	Sí
$minute	Sí	Sí	Sí	Sí	Sí
$month	Sí	Sí	Sí	Sí	Sí
$second	Sí	Sí	Sí	Sí	Sí
$week	Sí	Sí	Sí	Sí	Sí

Comando	3.6	4.0	5.0	8.0	Clúster elástico
$year	Sí	Sí	Sí	Sí	Sí

Operador literal

Comando	3.6	4.0	5.0	8.0	Clúster elástico
$literal	Sí	Sí	Sí	Sí	Sí

Operador de combinación

Comando	3.6	4.0	5.0	8.0	Clúster elástico
$mergeObjects	Sí	Sí	Sí	Sí	Sí

Operador natural

Comando	3.6	4.0	5.0	8.0	Clúster elástico
$natural	Sí	Sí	Sí	Sí	Sí

Operadores de establecimiento

Comando	3.6	4.0	5.0	8.0	Clúster elástico
$allElementsTrue	No	Sí	Sí	Sí	Sí
$anyElementTrue	No	Sí	Sí	Sí	Sí
$setDifference	No	Sí	Sí	Sí	Sí
$setEquals	Sí	Sí	Sí	Sí	Sí
$setIntersection	Sí	Sí	Sí	Sí	Sí
$setIsSubset	Sí	Sí	Sí	Sí	Sí
$setUnion	Sí	Sí	Sí	Sí	Sí
$setWindowFields	No	No	No	No	No

Operadores de etapa

Comando	3.6	4.0	5.0	8.0	Clúster elástico
$addFields	Sí	Sí	Sí	Sí	Sí
$bucket	No	No	No	Sí	No
$bucketAuto	No	No	No	No	

Comando	3.6	4.0	5.0	8.0	Clúster elástico
$changeStream	Sí	Sí	Sí	Sí	No
$collStats	No	Sí	Sí	Sí	No
$count	Sí	Sí	Sí	Sí	Sí
$currentOp	Sí	Sí	Sí	Sí	Sí
$facet	No	No	No	No	No
$geoNear	Sí	Sí	Sí	Sí	Sí
$graphLookup	No	No	No	No	No
$group	Sí	Sí	Sí	Sí	Sí
$indexStats	Sí	Sí	Sí	Sí	Sí
$limit	Sí	Sí	Sí	Sí	Sí
$listLocalSessions	No	No	No	No	No
$listSessions	No	No	No	No	No
$lookup	Sí	Sí	Sí	Sí	Sí
$match	Sí	Sí	Sí	Sí	Sí
$merge	-	-	No	Sí	No
$out	Sí	Sí	Sí	Sí	No
$planCacheStats	-	-	No	No	No

Comando	3.6	4.0	5.0	8.0	Clúster elástico
$project	Sí	Sí	Sí	Sí	Sí
$redact	Sí	Sí	Sí	Sí	Sí
$replaceRoot	Sí	Sí	Sí	Sí	Sí
$sample	Sí	Sí	Sí	Sí	Sí
$set	-	-	No	Sí	No
$setWindowFields	-	-	No	No	No
$skip	Sí	Sí	Sí	Sí	Sí
$sort	Sí	Sí	Sí	Sí	Sí
$sortByCount	No	No	No	No	No
$UnionWith	-	-	No	No	No
$unset	-	-	No	Sí	No
$unwind	Sí	Sí	Sí	Sí	Sí
$ Reemplazar con	No	No	No	Sí	No
$VectorSearch	No	No	No	Sí	No

Operadores de cadena

Comando	3.6	4.0	5.0	8.0	Clúster elástico
$concat	Sí	Sí	Sí	Sí	Sí
$indexOfBytes	Sí	Sí	Sí	Sí	Sí
$indexOfCP	Sí	Sí	Sí	Sí	Sí
$ltrim	No	Sí	Sí	Sí	No
$regexFind	-	-	Sí	Sí	No
$regexFindAll	-	-	Sí	Sí	No
$ RegexMatch	-	-	Sí	Sí	No
$ReplaceAll	-	-	Sí	Sí	No
$ ReplaceOne	-	-	Sí	Sí	No
$rtrim	No	Sí	Sí	Sí	No
$split	Sí	Sí	Sí	Sí	Sí
$strcasecmp	Sí	Sí	Sí	Sí	Sí
$strLenBytes	Sí	Sí	Sí	Sí	Sí
$strLenCP	Sí	Sí	Sí	Sí	Sí
$substr	Sí	Sí	Sí	Sí	Sí
$substrBytes	Sí	Sí	Sí	Sí	Sí
$substrCP	Sí	Sí	Sí	Sí	Sí

Comando	3.6	4.0	5.0	8.0	Clúster elástico
$toLower	Sí	Sí	Sí	Sí	Sí
$toUpper	Sí	Sí	Sí	Sí	Sí
$trim	No	Sí	Sí	Sí	No

Variables del sistema

Comando	3.6	4.0	5.0	8.0	Clúster elástico
$$CURRENT	No	No	No	No	No
$$DESCEND	Sí	Sí	Sí	Sí	Sí
$$KEEP	Sí	Sí	Sí	Sí	Sí
$$PRUNE	Sí	Sí	Sí	Sí	Sí
$$REMOVE	No	No	No	No	No
$$ROOT	Sí	Sí	Sí	Sí	Sí

Operador de búsqueda de texto

Comando	3.6	4.0	5.0	8.0	Clúster elástico
$meta	No	No	Sí	Sí	No
$search	No	No	Sí	Sí	No

Operadores de conversión de tipos

Comando	3.6	4.0	5.0	8.0	Clúster elástico
$convert	No	Sí	Sí	Sí	Sí
$es un número	-	-	No	No	No
$ a Bool	No	Sí	Sí	Sí	Sí
$toDate	No	Sí	Sí	Sí	Sí
$ a Decimal	No	Sí	Sí	Sí	Sí
$ a doble	No	Sí	Sí	Sí	Sí
$toInt	No	Sí	Sí	Sí	Sí
$ a Long	No	Sí	Sí	Sí	Sí
$toObjectId	No	Sí	Sí	Sí	Sí
$toString	No	Sí	Sí	Sí	Sí

Operadores de variables

Comando	3.6	4.0	5.0	8.0	Clúster elástico
$let	Sí	Sí	Sí	Sí	Sí
$map	Sí	Sí	Sí	Sí	Sí

Operadores misceláneos

Comando	3.6	4.0	5.0	8.0	Clúster elástico
$getField	-	-	No	No	No
$rand	-	-	No	Sí	No
$sampleRate	-	-	No	No	No

Tipos de datos

Comando	3.6	4.0	5.0	8.0	Clúster elástico
32-bit Integer (int)	Sí	Sí	Sí	Sí	Sí
Entero de 64 bits (largo)	Sí	Sí	Sí	Sí	Sí
Matriz	Sí	Sí	Sí	Sí	Sí
Datos Binary	Sí	Sí	Sí	Sí	Sí
Booleano	Sí	Sí	Sí	Sí	Sí
Date	Sí	Sí	Sí	Sí	Sí
DBPointer	No	No	No	No	No
DBRefs	No	No	No	No	No
Decimal128	Sí	Sí	Sí	Sí	Sí
Double	Sí	Sí	Sí	Sí	Sí
JavaScript	No	No	No	No	No

Comando	3.6	4.0	5.0	8.0	Clúster elástico
JavaScript(con alcance)	No	No	No	No	No
MaxKey	Sí	Sí	Sí	Sí	Sí
MinKey	Sí	Sí	Sí	Sí	Sí
Nulo	Sí	Sí	Sí	Sí	Sí
Objeto	Sí	Sí	Sí	Sí	Sí
ObjectId	Sí	Sí	Sí	Sí	Sí
Expresión regular	Sí	Sí	Sí	Sí	Sí
Cadena	Sí	Sí	Sí	Sí	Sí
Símbolo	No	No	No	No	No
Timestamp	Sí	Sí	Sí	Sí	Sí
Sin definir	No	No	No	No	No

Índices y propiedades de índices

Temas

- Índices
- Propiedades de índices

Índices

Comando	3.6	4.0	5.0	8.0	Clúster elástico
2dsphere	Sí	Sí	Sí	Sí	Sí
Índice 2d	No	No	No	No	No
Índice compuesto	Sí	Sí	Sí	Sí	Sí
Índice hash	No	No	No	No	No
Índice de varias claves	Sí	Sí	Sí	Sí	Sí
Índice de campo único	Sí	Sí	Sí	Sí	Sí
Índice de texto	No	No	Sí	Sí	No
Comodín	No	No	No	No	No

Propiedades de índices

Comando	3.6	4.0	5.0	8.0	Clúster elástico
Introducción	Sí	Sí	Sí	Sí	Sí
No distingue entre mayúsculas y minúsculas	No	No	No	Sí	No
Oculto	No	No	No	No	No

Comando	3.6	4.0	5.0	8.0	Clúster elástico
Parcial	No	No	Sí	Sí	No
Sparse	Sí	Sí	Sí	Sí	Sí
Texto	No	No	Sí	Sí	No
TTL	Sí	Sí	Sí	Sí	Sí
Unique	Sí	Sí	Sí	Sí	Sí
Vector	No	No	Sí	Sí	No

Inteligencia artificial generativa de Amazon DocumentDB

Amazon DocumentDB ofrece capacidades para permitir que los modelos de machine learning (ML) e inteligencia artificial (IA) generativa funcionen con los datos almacenados en Amazon DocumentDB en tiempo real. Los clientes ya no tienen que perder tiempo administrando una infraestructura independiente, escribiendo código para conectarse con otro servicio y duplicando datos de su base de datos principal.

Para obtener más información sobre la inteligencia artificial y cómo AWS puede satisfacer sus necesidades de IA, consulte este artículo sobre «Qué es».

Temas

- Aprendizaje automático sin código con Amazon SageMaker AI Canvas
- Búsqueda vectorial para Amazon DocumentDB

Aprendizaje automático sin código con Amazon SageMaker AI Canvas

Amazon SageMaker AI Canvas le permite crear sus propios AI/ML modelos sin tener que escribir una sola línea de código. Puede crear modelos de aprendizaje automático para casos de uso comunes, como la regresión y la previsión, y puede acceder a los modelos básicos y evaluarlos (FMs) desde Amazon Bedrock. También puede acceder al público FMs desde Amazon SageMaker AI JumpStart para la generación de contenido, la extracción de texto y el resumen de texto para respaldar las soluciones de IA generativa.

¿Cómo crear modelos de aprendizaje automático sin código con AI Canvas? SageMaker

Amazon DocumentDB ahora se integra con Amazon SageMaker AI Canvas para permitir el aprendizaje automático (ML) sin código con los datos almacenados en Amazon DocumentDB. Ahora puede crear modelos de machine learning para las necesidades de regresión y previsión y utilizar modelos fundacionales para resumir y generar contenido con datos almacenados en Amazon DocumentDB sin necesidad de escribir una sola línea de código.

SageMaker AI Canvas proporciona una interfaz visual que permite a los clientes de Amazon DocumentDB generar predicciones sin necesidad de AI/ML conocimientos ni escribir una sola

línea de código. Los clientes ahora pueden lanzar el espacio de trabajo de SageMaker AI Canvas desde Amazon DocumentDB Consola de administración de AWS, importarlos y unirlos para la preparación de datos y el entrenamiento de modelos. Los datos de Amazon DocumentDB ahora se pueden usar en SageMaker AI Canvas para crear y aumentar modelos con el fin de predecir la rotación de clientes, detectar fraudes, predecir fallos de mantenimiento, pronosticar métricas empresariales y generar contenido. Los clientes ahora pueden publicar y compartir información basada en el aprendizaje automático entre los equipos mediante la integración nativa de SageMaker AI Canvas con Quick Suite. Los canales de ingesta de datos de SageMaker AI Canvas se ejecutan en instancias secundarias de Amazon DocumentDB de forma predeterminada, lo que garantiza que el rendimiento de las cargas de trabajo de ingestión de aplicaciones SageMaker y AI Canvas no se vea afectado.

Los clientes de Amazon DocumentDB pueden empezar a utilizar SageMaker AI Canvas accediendo a la nueva página de la consola de aprendizaje automático sin código de Amazon DocumentDB y conectándose a espacios de trabajo de AI Canvas nuevos o disponibles. SageMaker

Configuración del dominio y el perfil de usuario de AI SageMaker

Puede conectarse a clústeres de Amazon DocumentDB desde dominios de SageMaker IA que se ejecutan en modo VPC únicamente. Al lanzar un dominio de SageMaker IA en su VPC, puede controlar el flujo de datos de sus entornos de SageMaker AI Studio y Canvas. Esto le permite restringir el acceso a Internet, monitorear e inspeccionar el tráfico mediante capacidades de AWS red y seguridad estándar y conectarse a otros AWS recursos a través de puntos de conexión de VPC. Consulte la sección Introducción y configuración de Amazon SageMaker AI Canvas en una VPC sin acceso a Internet, que se encuentra en la Guía para desarrolladores de Amazon SageMaker AI, para crear su dominio de SageMaker IA y conectarse a su clúster de Amazon DocumentDB. SageMaker

Configuración de los permisos de acceso de IAM para Amazon DocumentDB SageMaker y AI Canvas

Un usuario de Amazon DocumentDB que haya asociado `AmazonDocDBConsoleFullAccess` a su rol e identidad asociados puede acceder a la Consola de administración de AWS. Añada las siguientes acciones al rol o identidad antes mencionados para proporcionar acceso al aprendizaje automático sin código con Amazon SageMaker AI Canvas.

```
"sagemaker:CreatePresignedDomainUrl",
"sagemaker:DescribeDomain",
"sagemaker:ListDomains",
```

```
"sagemaker:ListUserProfiles"
```

Creación de usuarios y roles de bases de datos para SageMaker AI Canvas

Puede restringir el acceso a las acciones que los usuarios pueden hacer en bases de datos mediante el control de acceso basado en roles (RBAC) en Amazon DocumentDB. RBAC funciona otorgando uno o más roles a un usuario. Estos roles determinan las operaciones que un usuario puede realizar en los recursos de la base de datos.

Como usuario de Canvas, se conecta a una base de datos de Amazon DocumentDB con credenciales de nombre de usuario y contraseña. Puede crear una base de datos user/role para un usuario de Canvas que tenga acceso de lectura a las bases de datos específicas mediante la funcionalidad RBAC de Amazon DocumentDB.

Por ejemplo, utilice la operación `createUser`:

```
db.createUser({
user: "canvas_user",
pwd: "<insert-password>",
roles: [{role: "read", db: "sample-database-1"}]
})
```

Esto crea un `canvas_user` que tiene permisos de lectura en la base de datos `sample-database-1`. Los analistas de Canvas pueden utilizar esta credencial para acceder a los datos del clúster de Amazon DocumentDB. Consulte Acceso a la base de datos mediante el control de acceso basado en roles para obtener más información.

Regiones disponibles

La integración sin código está disponible en las regiones en las que se admiten Amazon DocumentDB y SageMaker Amazon AI Canvas. Las regiones son:

- us-east-1 (Norte de Virginia)
- us-east-2 (Ohio)
- us-west-2 (Oregón)
- ap-northeast-1 (Tokio)
- ap-northeast-2 (Seúl)

- ap-south-1 (Mumbai)
- ap-southeast-1 (Singapur)
- ap-southeast-2 (Sídney)
- eu-central-1 (Fráncfort)
- eu-west-1 (Irlanda)

Consulte Amazon SageMaker AI Canvas en la Guía para desarrolladores de Amazon SageMaker AI para conocer la disponibilidad regional más reciente.

Búsqueda vectorial para Amazon DocumentDB

La búsqueda vectorial es un método utilizado en el machine learning para encontrar puntos de datos similares a un punto de datos determinado mediante la comparación de sus representaciones vectoriales mediante métricas de distancia o similitud. Cuanto más cerca estén los dos vectores del espacio vectorial, más parecidos se considerarán los elementos subyacentes. Esta técnica ayuda a captar el significado semántico de los datos. Este enfoque es útil en diversas aplicaciones, como los sistemas de recomendación, el procesamiento del lenguaje natural y el reconocimiento de imágenes.

La búsqueda vectorial para Amazon DocumentDB combina la flexibilidad y la amplia capacidad de consulta de una base de datos de documentos basada en JSON con la potencia de la búsqueda vectorial. Si desea utilizar sus datos actuales de Amazon DocumentDB o una estructura de datos de documentos flexible para crear casos de uso de machine learning e IA generativa, como la experiencia de búsqueda semántica, recomendación de productos, personalización, chatbots, detección de fraudes y detección de anomalías, la búsqueda vectorial para Amazon DocumentDB es la opción ideal para usted. La búsqueda vectorial está disponible en los clústeres basados en instancias de Amazon DocumentDB 5.0.

Temas

- Inserción de vectores
- Creación de un índice vectorial
- Obtención de una definición de índice
- Consulta de vectores
- Características y limitaciones
- Prácticas recomendadas

Inserción de vectores

Para insertar vectores en la base de datos de Amazon DocumentDB, puede utilizar los métodos de inserción existentes:

Ejemplo

En el siguiente ejemplo, se crea una colección de cinco documentos dentro de una base de datos de prueba. Cada documento incluye dos campos: el nombre del producto y su incrustación vectorial correspondiente.

```
db.collection.insertMany([
  {"product_name": "Product A", "vectorEmbedding": [0.2, 0.5, 0.8]},
  {"product_name": "Product B", "vectorEmbedding": [0.7, 0.3, 0.9]},
  {"product_name": "Product C", "vectorEmbedding": [0.1, 0.2, 0.5]},
  {"product_name": "Product D", "vectorEmbedding": [0.9, 0.6, 0.4]},
  {"product_name": "Product E", "vectorEmbedding": [0.4, 0.7, 0.2]}
]);
```

Creación de un índice vectorial

Amazon DocumentDB admite los métodos de indexación Jerarchical Navigable Small World (HNSW) y de indexación de archivos invertidos con compresión plana (). IVFFlat Un IVFFlat índice segrega los vectores en listas y, posteriormente, busca en un subconjunto seleccionado de las listas más cercanas al vector de consulta. Por otro lado, un índice HNSW organiza los datos vectoriales en un gráfico de varias capas. Si bien HNSW tiene tiempos de creación más lentos en comparación con HNSW IVFFlat, ofrece un mejor rendimiento y recuperación de las consultas. Por el contrario IVFFlat, HNSW no implica ningún paso de entrenamiento, lo que permite generar el índice sin ninguna carga inicial de datos. En la mayoría de los casos de uso, recomendamos utilizar el tipo de índice HNSW para la búsqueda vectorial.

Si no crea un índice vectorial, Amazon DocumentDB hacer una búsqueda exacta del vecino más cercano, lo que garantiza una recuperación perfecta. Sin embargo, en los escenarios de producción, la velocidad es crucial. Recomendamos utilizar índices vectoriales, que pueden cambiar un poco de memoria por mejorar la velocidad. Es importante tener en cuenta que agregar un índice vectorial puede generar resultados de consulta diferentes.

Plantillas

Puede usar las siguientes plantillas de `createIndex` o `runCommand` para crear un índice vectorial en un campo vectorial:

Using createIndex

En algunos controladores, como mongosh y Java, el uso de los parámetros `vectorOptions` de `createIndex` puede provocar un error. En estos casos, recomendamos utilizar `runCommand`:

```
db.collection.createIndex(
  { "<vectorField>": "vector" },
  { "name": "<indexName>",
    "vectorOptions": {
      "type": " <hnsw> | <ivfflat> ",
      "dimensions": <number_of_dimensions>,
      "similarity": " <euclidean> | <cosine> | <dotProduct> ",
      "lists": <number_of_lists> [applicable for IVFFlat],
      "m": <max number of connections> [applicable for HNSW],
      "efConstruction": <size of the dynamic list for index build> [applicable for
 HNSW]
    }
  }
);
```

Using runCommand

En algunos controladores, como mongosh y Java, el uso de los parámetros `vectorOptions` de `createIndex` puede provocar un error. En estos casos, recomendamos utilizar `runCommand`:

```
db.runCommand(
  { "createIndexes": "<collection>",
  "indexes": [{
      key: { "<vectorField>": "vector" },
      vectorOptions: {
          type: " <hnsw> | <ivfflat> ",
          dimensions: <number of dimensions>,
          similarity: " <euclidean> | <cosine> | <dotProduct> ",
          lists: <number_of_lists> [applicable for IVFFlat],
          m: <max number of connections> [applicable for HNSW],
          efConstruction: <size of the dynamic list for index build> [applicable for
 HNSW]
          },
      name: "myIndex"
      }]
```

```
  }
);
```

Parámetro	Requisito	Tipo de datos:	Description (Descripción)	Valores
`name`	opcional	cadena	Especifica el nombre del índice.	Alfanumérico
`type`	opcional		Especifica el tipo de índice.	Compatible: hnsw o ivfflat Valor predeterminado: HNSW (con el parche del motor a partir de la versión 3.0.4574)
`dimensions`	obligatorio	entero	Especifica el número de dimensiones de los datos vectoriales.	Máximo de 2000 dimensiones.
`similarity`	obligatorio	cadena	Especifica la métrica de distancia utilizada para el cálculo de similitud.	• **`euclidean`** • **`cosine`** • **`dotProduct`**
`lists`	necesario para IVFFlat	entero	Especifica el número de clústeres que el IVFFlat índice	Mínimo: 1 Máximo: consulte la tabla de listas por

Parámetro	Requisito	Tipo de datos:	Description (Descripción)	Valores
			utiliza para agrupar los datos vectoriales. La configuración recomendada es el número de documentos/1000 para un máximo de un millón de documentos y `sqrt(# of documents)` para más de un millón de documentos.	tipo de instancia que aparece en Características y limitaciones a continuación.
`m`	opcional	entero	Especifica el número máximo de conexiones para un índice HNSW	Predeterminado: 16 Rango: [2, 100]

Parámetro	Requisito	Tipo de datos:	Description (Descripción)	Valores
efConstruction	opcional	entero	Especifica el tamaño de la lista dinámica de candidatos para construir el gráfico del índice de HNSW. `efConstruction` debe ser mayor o igual que (2 * m)	Predeterminado: 64 Rango [4, 1000]

Es importante que establezca adecuadamente el valor de los subparámetros, como `lists` para IVFFlat `m` y `efConstruction` para HNSW, ya que esto afectará a la precisión/recuperación, al tiempo de creación y al rendimiento de la búsqueda. Un valor de lista más alto aumenta la velocidad de la consulta, ya que reduce el número de vectores de cada lista, lo que se traduce en regiones más pequeñas. Sin embargo, un tamaño de región más pequeño puede provocar más errores de recuperación, lo que se traduce en una menor precisión. En el caso de HNSW, aumentar el valor `m` y `efConstruction` aumenta la precisión, pero también se incrementa el tiempo y el tamaño de creación del índice. Consulte los siguientes ejemplos:

Ejemplos

HNSW

```
db.collection.createIndex(
  { "vectorEmbedding": "vector" },
  { "name": "myIndex",
    "vectorOptions": {
      "type": "hnsw",
      "dimensions": 3,
      "similarity": "euclidean",
      "m": 16,
      "efConstruction": 64
    }
```

```
  }
);
```

IVFFlat

```
db.collection.createIndex(
  { "vectorEmbedding": "vector" },
  { "name": "myIndex",
    "vectorOptions": {
      "type": "ivfflat",
      "dimensions": 3,
      "similarity": "euclidean",
      "lists":1
    }
  }
)
```

Obtención de una definición de índice

Puede ver los detalles de los índices, incluidos los índices vectoriales, mediante el comando `getIndexes`:

Ejemplo

```
db.collection.getIndexes()
```

Ejemplo de salida

```
[
 {
  "v" : 4,
  "key" : {
   "_id" : 1
  },
  "name" : "_id_",
  "ns" : "test.collection"
 },
 {
  "v" : 4,
  "key" : {
   "vectorEmbedding" : "vector"
```

```
  },
  "name" : "myIndex",
  "vectorOptions" : {
   "type" : "ivfflat",
   "dimensions" : 3,
   "similarity" : "euclidean",
   "lists" : 1
  },
  "ns" : "test.collection"
 }
]
```

Consulta de vectores

Amazon DocumentDB admite dos operadores de búsqueda vectorial para consultar vectores:

Operador de búsqueda vectorial clásico

Utilice la siguiente plantilla para consultar un vector:

```
db.collection.aggregate([
  {
    $search: {
      "vectorSearch": {
        "vector": <query vector>,
        "path": "<vectorField>",
        "similarity": "<distance metric>",
        "k": <number of results>,
        "probes":<number of probes> [applicable for IVFFlat],
        "efSearch":<size of the dynamic list during search> [applicable for HNSW]
      }
    }
  }
]);
```

Parámetro	Requisito	Tipo	Description (Descripción)	Valores
vectorSearch	obligatorio	operador	Se utiliza dentro del comando $search para	

Parámetro	Requisito	Tipo	Description (Descripción)	Valores
			consultar los vectores.	
vector	obligatorio	array	Indica el vector de consulta que se utilizará para buscar vectores similares.	
path	obligatorio	cadena	Define el nombre del campo vectorial.	
k	obligatorio	entero	Especifica el número de resultados que devuelve la búsqueda.	
similarity	obligatorio	cadena	Especifica la métrica de distancia utilizada para el cálculo de similitud.	• **euclidean** • **cosine** • **dotProduct**

Parámetro	Requisito	Tipo	Description (Descripción)	Valores
`probes`	opcional	entero	El número de clústeres que desea que inspeccione la búsqueda vectorial. Un valor más alto proporciona una mejor recuperación a costa de la velocidad. Se puede establecer en función del número de listas para la búsqueda exacta del vecino más cercano (momento en el que el planificador no utilizará el índice). La configuración recomendada para iniciar el ajuste preciso es `sqrt(# of lists)`.	Valor predeterminado: 1

Parámetro	Requisito	Tipo	Description (Descripción)	Valores
`efSearch`	opcional	entero	Especifica el tamaño de la lista dinámica de candidatos que el índice de HNSW utiliza durante la búsqueda. Un valor más alto de `efSearch` proporciona una mejor recuperación a costa de la velocidad.	Predeterminado: 40 Rango: [1, 1000]

Es importante ajustar con precisión el valor de `efSearch` (HNSW) o `probes` (IVFFlat) para lograr el rendimiento y la precisión deseados. Vea los siguientes ejemplos de operaciones:

HNSW

```
db.collection.aggregate([
  {
    $search: {
      "vectorSearch": {
        "vector": [0.2, 0.5, 0.8],
        "path": "vectorEmbedding",
        "similarity": "euclidean",
        "k": 2,
        "efSearch": 40
      }
    }
  }
]);
```

IVFFlat

```
db.collection.aggregate([
  {
    $search: {
      "vectorSearch": {
        "vector": [0.2, 0.5, 0.8],
        "path": "vectorEmbedding",
        "similarity": "euclidean",
        "k": 2,
        "probes": 1
      }
    }
  }
]);
```

Ejemplo de salida

La salida de esta operación será similar a lo que se indica a continuación:

```
{ "_id" : ObjectId("653d835ff96bee02cad7323c"), "product_name" : "Product A",
 "vectorEmbedding" : [ 0.2, 0.5, 0.8 ] }
{ "_id" : ObjectId("653d835ff96bee02cad7323e"), "product_name" : "Product C",
 "vectorEmbedding" : [ 0.1, 0.2, 0.5 ] }
```

$vectorSearchoperador (disponible en Amazon DocumentDB 8.0 en adelante)

Utilice la siguiente plantilla para consultar un vector:

```
db.collection.aggregate([
{
  "$vectorSearch": {
    "exact": true | false,
    "index": "<index-name>" [supports only HNSW index],
    "limit": <number-of-results> [same as k],
    "path": "<vector field-to-search>",
    "queryVector": <array-of-numbers>,
    "numCandidates": <number-of-candidates> [same as efSearch],
  }
}])
```

Características y limitaciones

Compatibilidad de versiones

- La búsqueda vectorial para Amazon DocumentDB solo está disponible en los clústeres basados en instancias de Amazon DocumentDB 5.0+.

Vectores

- Amazon DocumentDB puede indexar vectores de hasta 2000 dimensiones. Sin embargo, se pueden almacenar hasta 16 000 dimensiones sin un índice.

Índices

- Para la creación de IVFFlat índices, la configuración recomendada para el parámetro de listas es el número de documentos/1000 para un máximo de 1 millón de documentos y para más de 1 millón de documentos. `sqrt(# of documents)` Debido al límite de memoria de trabajo, Amazon DocumentDB admite un determinado valor máximo del parámetro de listas en función del número de dimensiones. Como referencia, en la siguiente tabla se proporcionan los valores máximos del parámetro de listas para vectores de 500, 1000 y 2000 dimensiones:

Tipo de instancia	Listas con 500 dimensiones	Listas con 1000 dimensiones	Listas con 2000 dimensiones
t3.med	372	257	150
r5.l	915	741	511
r5.xl	1.393	1.196	901
r5.2xl	5.460	5.230	4.788
r5.4xl	7.842	7.599	7.138
r5.8xl	11.220	10.974	10.498
r5.12xl	13.774	13.526	13.044
r5.16xl	15.943	15.694	15.208

Tipo de instancia	Listas con 500 dimensiones	Listas con 1000 dimensiones	Listas con 2000 dimensiones
r5.24xl	19.585	19.335	18.845

- Los índices vectoriales no admiten otras opciones de índice, como `compound`, `sparse` o `partial`.
- La compilación de índices paralelos no es compatible con el índice HNSW en Amazon DocumentDB 5.0.

Consulta vectorial

- Para una consulta de búsqueda vectorial, es importante afinar los parámetros, por ejemplo, `probes` o `efSearch`, para obtener resultados óptimos. Cuanto mayor sea el valor del parámetro `probes` o `efSearch`, mayor será la recuperación y menor será la velocidad. La configuración recomendada para iniciar el ajuste preciso del parámetro de sondas es `sqrt(# of lists)`.

Prácticas recomendadas

Descubra las prácticas recomendadas para trabajar con la búsqueda vectorial en Amazon DocumentDB. Esta sección se actualiza continuamente a medida que se identifican nuevas prácticas recomendadas.

- La creación del índice de archivos invertidos con compresión plana (IVFFlat) implica agrupar y organizar los puntos de datos en función de las similitudes. Por lo tanto, para que un índice sea más eficaz, le recomendamos que cargue al menos algunos datos antes de crearlo.
- Para consultas de búsqueda vectorial, es importante afinar los parámetros, por ejemplo, `probes` o `efSearch`, para obtener resultados óptimos. Cuanto mayor sea el valor del parámetro `probes` o `efSearch`, mayor será la recuperación y menor será la velocidad. La configuración recomendada para empezar a afinar el parámetro `probes` es `sqrt(lists)`.

Recursos

- Búsqueda vectorial: entrada de novedades del blog
- Ejemplo de código de búsqueda semántica
- Ejemplos de códigos de búsqueda vectorial de Amazon DocumentDB

Migración a Amazon DocumentDB

Amazon DocumentDB es una base de datos administrada que es compatible con la API de MongoDB. Puede migrar sus datos a Amazon DocumentDB desde bases de datos de MongoDB que se ejecuten localmente o en Amazon Elastic Compute Cloud (Amazon EC2) mediante el proceso que se detalla en esta sección.

Temas

- Migración a Amazon DocumentDB mediante AWS Database Migration Service (DMS): guía de inicio rápido
- Runbook de migración de Amazon DocumentDB
- Migración desde Couchbase Server

Migración a Amazon DocumentDB mediante AWS Database Migration Service (DMS): guía de inicio rápido

Temas

- Preparación del origen de DMS
- Configuración de DMS
- Habilitación de la compresión de DocumentDB
- Creación de una tarea de replicación
- Monitorear el progreso
- Información adicional

Preparación del origen de DMS

Consulte Habilitación de flujos de cambios para habilitar los flujos de cambios de DocumentDB o habilitar el oplog de MongoDB para admitir la captura de datos de cambio (CDC) de DMS.

- El origen de DMS debe retener todos los cambios en curso hasta que se complete la carga completa de DMS para todas las colecciones incluidas.

- Los flujos de cambios de DocumentDB se basan en el tiempo. Asegúrese de que la configuración de `change_stream_log_retention_duration` sea lo suficientemente grande como para cubrir el tiempo necesario para concluir la carga completa.
- El oplog de MongoDB tiene un tamaño fijo. Asegúrese de que tiene el tamaño adecuado para admitir todas las operaciones durante la carga completa.

Configuración de DMS

Cree puntos de conexión de instancia, origen y destino de DMS y pruebe cada punto de conexión.

Habilitación de la compresión de DocumentDB

Para habilitar la compresión, adjunte un grupo de parámetros personalizado al clúster de DocumentDB y actualice el parámetro default_collection_compression a habilitado. Para obtener más información, consulte Gestión de la compresión de documentos a nivel de colección.

Creación de una tarea de replicación

1. En la consola de DMS, en el panel de navegación, elija Migrar o replicar y, a continuación, elija Tareas.
2. Seleccione Crear tarea.
3. En la página Crear tarea, en la sección Configuración de tareas:
   - Introduzca un Identificador de tarea único y significativo (por ejemplo, «mongodb-docdb-replication»).
   - Elija el punto de conexión de origen que creó anteriormente en el menú desplegable de Punto de conexión de la base de datos de origen.
   - Elija el punto de conexión de destino que creó anteriormente en el menú desplegable de Punto de conexión de la base de datos de destino.
   - En Tipo de tarea, elija Migrar y replicar.
4. En la sección Configuración:
   - En Registros de tareas, marque la casilla Activar registros de CloudWatch.
   - En Modo de edición (en la parte superior de la sección), elija el editor JSON y defina los siguientes atributos:

- Establezca `ParallelApplyThreads` en 5 (en `TargetMetadata`). Esto permite ~1000 operaciones de insertar/actualizar/eliminar por segundo en la CDC.
- Establezca `MaxFullLoadSubTasks` en 16 (en `FullLoadSettings`). Considere aumentar el valor en función del tamaño de la instancia.
- Para colecciones grandes (más de 100 GB), habilite la partición automática (en Correspondencia de tablas y en el atributo `parallel-load`):
  - «type»: «partitions-auto»
  - «number-of-partitions»: 16

Monitorear el progreso

Use la consola de AWS DMS o cree un panel de control personalizado (herramienta de panel de control) para realizar un seguimiento de la migración. Debe concentrarse en las siguientes métricas:

- FullloadThroughputBandWidthTarget: mide el ancho de banda de la red (en KB/segundo) que utiliza DMS para transferir datos a la base de datos de destino durante la fase de carga completa de la migración.
- CDCLatencyTarget: mide el tiempo transcurrido (en segundos) entre el momento en que se produce un cambio en la base de datos de origen y el momento en que ese cambio se aplica a la base de datos de destino.
- CDCThroughputRowsTarget: mide el número de filas por segundo que DMS aplica a la base de datos de destino durante la fase de replicación en curso de la migración.

Información adicional

Para obtener más información acerca de Amazon DocumentDB y AWS DMS, consulte:

- Runbook de migración de Amazon DocumentDB
- Migración desde MongoDB a Amazon DocumentDB

Runbook de migración de Amazon DocumentDB

Este manual proporciona una guía completa para migrar una base de datos de MongoDB a Amazon DocumentDB mediante (DMS). AWS Database Migration Service Está diseñado para ayudar a los

administradores de bases de datos, ingenieros de nube y desarrolladores durante todo el proceso de migración, desde el descubrimiento inicial hasta la validación posterior a la end-to-end migración.

Dadas las diferencias en la implementación y las características compatibles entre MongoDB y Amazon DocumentDB, en este runbook se hace hincapié en un enfoque estructurado y sistemático. Se describen las evaluaciones esenciales previas a la migración, se destacan las consideraciones de compatibilidad y se detallan las tareas clave necesarias para garantizar una migración correcta con un mínimo de interrupciones.

El runbook se organiza en los siguientes temas:

- Compatibilidad: conozca las características y los tipos de datos de MongoDB compatibles con Amazon DocumentDB e identifique posibles incompatibilidades.
- Detección de la carga de trabajo— Analice las cargas de trabajo de MongoDB existentes, read/write incluidos los patrones, los volúmenes de datos y las líneas base de rendimiento.
- Migración de índices: analice las estrategias para extraer y transformar los índices de MongoDB para obtener un rendimiento óptimo en Amazon DocumentDB.
- Migración de usuario: detalle el enfoque para migrar los usuarios, los roles y los controles de acceso de las bases de datos a Amazon DocumentDB.
- Migración de datos— Describa varios métodos para la migración de datos AWS DMS, incluida la captura de datos a plena carga y cambios (CDC).
- Supervisión: detalle varios enfoques de supervisión cuando haga una migración mediante DMS o herramientas nativas.
- Validación: proporcione procedimientos para las comprobaciones de integridad de los datos, la validación funcional y la comparación del rendimiento después de la migración.

Si se siguen las instrucciones de este runbook, los equipos pueden garantizar una transición fluida, segura y eficiente a Amazon DocumentDB, a la vez que conservan la funcionalidad de la aplicación y minimizan los riesgos.

Compatibilidad

Temas

- Compatibilidad de características básicas
- Herramienta de evaluación de compatibilidad de Amazon DocumentDB

Cuando se realiza una migración de MongoDB a Amazon DocumentDB, es esencial realizar una evaluación inicial exhaustiva y comprobar la compatibilidad de las características para que la migración se lleve a cabo correctamente. Este proceso comienza con un inventario completo de las características de MongoDB, incluidos los operadores de canalización de agregación, los patrones de consulta, los índices y los modelos de datos.

Dado que Amazon DocumentDB es compatible con las API de MongoDB 3.6, 4.0 y 5.0, es posible que sea necesario refactorizar las aplicaciones que utilizan características específicas de MongoDB más recientes. Las áreas críticas que se deben evaluar incluyen los mecanismos de partición (Amazon DocumentDB utiliza un enfoque diferente), las implementaciones de transacciones, la funcionalidad de los flujos de cambios y los tipos de índices (especialmente los índices dispersos y parciales).

Las características de rendimiento también difieren, ya que Amazon DocumentDB está optimizada para cargas de trabajo empresariales con un rendimiento predecible. Las pruebas deben incluir la ejecución de cargas de trabajo representativas en ambos sistemas para identificar los patrones de consulta que puedan requerir optimización.

Durante la fase de evaluación, es importante supervisar los planes de ejecución para detectar posibles brechas de rendimiento. Esto ayuda a crear una hoja de ruta de migración clara, ya que identifica los cambios necesarios en las aplicaciones y establece plazos realistas para una transición fluida.

Compatibilidad de características básicas

Soporte de características integral

- Operaciones CRUD: disfrute de una compatibilidad total con todas las operaciones básicas de creación, lectura, actualización y eliminación, incluidos los operadores masivos y de consulta, lo que proporciona una compatibilidad perfecta entre aplicaciones.
- Amplias capacidades de indexación: aproveche el soporte integral para índices de un solo campo, compuestos, TTL, parciales, dispersos y de 2dsphere para optimizar el rendimiento de sus consultas y los índices de texto (versión 5) para las búsquedas basadas en texto.
- Replicación de nivel empresarial: benefíciese de un sólido mecanismo de conmutación por error automática con réplicas de lectura para obtener una alta disponibilidad superior sin sobrecargas operativas.

- Soluciones de respaldo avanzadas: descanse tranquilo con un sistema de respaldo automatizado que incluye Point-in-Time recuperación (PITR) e instantáneas manuales bajo demanda para proteger los datos.

Funciones integradas y mejoradas AWS

- Agregación simplificada: aproveche las etapas de agregación más utilizadas (`$match`, `$group`, `$sort`, `$project`, etc.) con un rendimiento optimizado para las cargas de trabajo empresariales.
- Soporte de transacciones: implemente transacciones con documentos y colecciones múltiples, lo que resulta perfecto para la mayoría de las necesidades de las aplicaciones empresariales.
- Seguimiento de datos en tiempo real: habilite los flujos de cambios con un simple comando y aumente el período de retención del flujo de cambios mediante una sencilla configuración de grupos de parámetros para supervisar los cambios en los datos en tiempo real.
- Servicios basados en la ubicación: implemente aplicaciones geoespaciales compatibles con los índices de operador y de 2dsphere de `$geoNear`.
- Capacidades de búsqueda de texto: utilice la funcionalidad integrada de búsqueda de texto para las necesidades de detección de contenido.

Ventajas de la arquitectura moderna

- Diseño nativo de la nube: disfrute de una arquitectura AWS optimizada que reemplaza las funciones antiguas, como MapReduce las operaciones de canalización de agregación más eficientes.
- Seguridad mejorada: aproveche las ventajas de la autenticación con AWS Identity and Access Management certificado (IAM), SCRAM-SHA-1, SCRAM-SHA-256, X.509 y autenticación basada en contraseñas.
- Rendimiento predecible: disfrute de un rendimiento uniforme optimizado específicamente para las cargas de trabajo empresariales.

Para obtener una descripción general completa de las capacidades de Amazon DocumentDB, consulte APIsMongoDB, operaciones y tipos de datos compatibles en Amazon DocumentDB y Diferencias funcionales: Amazon DocumentDB y MongoDB para maximizar el potencial de su base de datos.

Amazon DocumentDB no es compatible con todos los índices que ofrece MongoDB. Proporcionamos una herramienta de indexación gratuita para comprobar la compatibilidad. Recomendamos utilizar la herramienta de indexación para evaluar la incompatibilidad y planificar las soluciones alternativas en consecuencia.

Herramienta de evaluación de compatibilidad de Amazon DocumentDB

La herramienta de compatibilidad de MongoDB a Amazon DocumentDB es una utilidad de código abierto GitHub que ayuda a evaluar la compatibilidad de las cargas de trabajo de MongoDB con Amazon DocumentDB mediante el análisis de los registros de MongoDB o del código fuente de la aplicación.

Características principales

- Identifica los patrones de uso de la API de MongoDB en su carga de trabajo.
- Señala posibles problemas de compatibilidad antes de la migración.
- Genera informes de compatibilidad detallados con recomendaciones.
- Está disponible como una utilidad independiente que se puede ejecutar localmente.

Métodos de evaluación

Evaluación basada en registros

- Ventajas:
  - Captura el comportamiento real del tiempo de ejecución y los patrones de consulta.
  - Identifica las frecuencias de uso y las características de rendimiento del mundo real.
  - Detecta consultas dinámicas que podrían no estar visibles en el código fuente.
  - No requiere el acceso al código fuente de la aplicación.
- Desventajas:
  - Requiere acceso a los registros de MongoDB con la creación de perfiles habilitada.
  - Captura solamente las operaciones que se produjeron durante el período de registro.
  - Es posible que pase por alto las características que se utilizan con poca frecuencia o las cargas de trabajo estacionales.

Análisis del código fuente

- Ventajas:
  - Brinda cobertura completa de todas las posibles operaciones de MongoDB en el código base.
  - Puede identificar problemas en las rutas de código que se ejecutan con poca frecuencia.
  - Detecta la lógica del lado del cliente que podría verse afectada por las diferencias en Amazon DocumentDB.
  - No requiere que se ejecute la aplicación para realizar la evaluación.
- Desventajas:
  - Puede marcar un código que existe, pero que nunca se ejecuta en producción.
  - Requiere acceso al código fuente completo de la aplicación.
  - Tiene capacidad limitada para analizar consultas creadas dinámicamente.

Para obtener los mejores resultados, recomendamos utilizar ambos métodos de evaluación siempre que sea posible para obtener una visión completa de los problemas de compatibilidad antes de la migración.

Detección de la carga de trabajo

La migración de MongoDB a Amazon DocumentDB requiere un conocimiento profundo de la carga de trabajo de la base de datos existente. La detección de la carga de trabajo es el proceso de analizar los patrones de uso de la base de datos, las estructuras de datos, el rendimiento de las consultas y las dependencias operativas para garantizar una transición fluida con una interrupción mínima. En esta sección se describen los pasos clave que implica la detección de cargas de trabajo para facilitar una migración eficaz de MongoDB a Amazon DocumentDB.

Temas

- Evaluación de la implementación de MongoDB existente
- Identificación de diferencias en los modelos de datos
- Análisis de consultas y rendimiento
- Revisión de seguridad y control de acceso
- Consideraciones operativas y de supervisión

Evaluación de la implementación de MongoDB existente

Antes de la migración, es fundamental evaluar el entorno actual de MongoDB, que incluye:

- Arquitectura del clúster: identifique la cantidad de nodos, los conjuntos de réplicas y las configuraciones de partición. Cuando migra de MongoDB a Amazon DocumentDB, es importante comprender la configuración de partición de MongoDB, ya que Amazon DocumentDB no admite la partición controlada por el usuario. Las aplicaciones diseñadas para un entorno de MongoDB con partición necesitarán cambios en la arquitectura, ya que Amazon DocumentDB utiliza un enfoque de escalado diferente con su arquitectura basada en el almacenamiento. Tendrá que adaptar su estrategia de distribución de datos y, posiblemente, consolidar las colecciones con partición cuando pase a Amazon DocumentDB.
- Almacenamiento y volumen de datos: mida el tamaño total de los datos y el tamaño del índice de su clúster. Complemente esto con la herramienta de revisión del oplog para comprender los patrones de escritura y la velocidad de crecimiento de los datos. Para obtener más información acerca del dimensionamiento de su clúster, consulte Determinación del tamaño de las instancias.
- Patrones de carga de trabajo: analice el rendimiento de lectura y escritura, la frecuencia de ejecución de las consultas y la eficiencia de la indexación.
- Dependencias operativas: documente todas las aplicaciones, los servicios y las integraciones que se basan en MongoDB.

Identificación de diferencias en los modelos de datos

Si bien Amazon DocumentDB es compatible con MongoDB, existen diferencias en las características compatibles, como:

- Transacciones: Amazon DocumentDB admite transacciones ACID, pero con algunas Limitaciones.
- Diseño de esquemas: asegúrese de que las estructuras de los documentos, los documentos incrustados y las referencias se ajusten a las prácticas recomendadas de Amazon DocumentDB.

Análisis de consultas y rendimiento

Comprender el comportamiento de las consultas ayuda a optimizar el rendimiento de la migración y después de la migración. Las siguientes son áreas clave que se deben analizar:

- Consultas lentas: identifique las consultas con un tiempo de ejecución elevado mediante las herramientas de creación de perfiles de MongoDB.
- Patrones de consulta: clasifique los tipos de consultas más frecuentes, incluidas las operaciones CRUD y las agregaciones.

- Uso de índices: evalúe si los índices se utilizan de forma eficaz o si es necesario optimizarlos en Amazon DocumentDB. Para evaluar el uso de los índices y optimizar el rendimiento en Amazon DocumentDB, use la etapa de canalización de agregación de `$indexStats` en combinación con el método de `explain()` en sus consultas críticas. Comience por ejecutar `db.collection.aggregate([{$indexStats{}}])` para identificar qué índices se están utilizando. Puede realizar un análisis más detallado ejecutando las consultas más frecuentes con `explainPlan`.
- Concurrencia y distribución de la carga de trabajo: evalúe las relaciones de lectura y escritura, la agrupación de conexiones y los cuellos de botella en el rendimiento.

Revisión de seguridad y control de acceso

Autenticación y autorización

- RBAC de MongoDB a IAM y RBAC de Amazon DocumentDB: asigne los usuarios y roles de control de acceso basado en roles de MongoDB a las políticas (IAM) y a los usuarios de autenticación SCRAM de Amazon DocumentDB. AWS Identity and Access Management
- Estrategia de migración de usuarios: planifique la migración de los usuarios de bases de datos, los roles personalizados y los privilegios a los mecanismos de autenticación compatibles con Amazon DocumentDB.
- Diferencias de privilegios: identifique los privilegios de MongoDB sin equivalentes directos de Amazon DocumentDB (por ejemplo, roles de administración de clústeres).
- Autenticación de aplicaciones: actualice las cadenas de conexión y la administración de credenciales para las políticas de contraseñas de Amazon DocumentDB. Puede usar el administrador de secretos para almacenar sus credenciales y rotar las contraseñas.
- Administración de cuentas de servicio: establezca procesos para AWS Secrets Manager administrar las credenciales de las cuentas de servicio en.
- Implementación de privilegios mínimos: revise y perfeccione los controles de acceso para implementar los principios de privilegios mínimos en el nuevo entorno.

Cifrado

Asegúrese de que el cifrado en reposo y en tránsito se ajuste a los requisitos de conformidad.

Configuración de red

Planifique la configuración de la nube privada virtual (VPC) y las reglas de los grupos de seguridad.

Consideraciones operativas y de supervisión

Para mantener la fiabilidad del sistema, la detección de la carga de trabajo también debe incluir lo siguiente:

- Estrategia de copia de seguridad y restauración: evalúe los métodos de copia de seguridad existentes y las capacidades de copia de seguridad de Amazon DocumentDB.
- AWS Backup integración: aproveche la administración centralizada AWS Backup de copias de seguridad en todos AWS los servicios, incluido Amazon DocumentDB.
- CloudWatch métricas: asigne las métricas de monitoreo de MongoDB a las métricas de Amazon DocumentDB para la CPU, la memoria, las conexiones y el almacenamiento. CloudWatch
- Información sobre rendimiento: implemente la Información de rendimiento de Amazon DocumentDB para visualizar la carga de la base de datos y analizar los problemas de rendimiento con análisis de consultas detallados.
- Generador de perfiles: configure el generador de perfiles de Amazon DocumentDB para capturar operaciones de ejecución lenta (similar al generador de perfiles de MongoDB, pero con ajustes específicos de Amazon DocumentDB).
  - Realice la habilitación mediante grupos de parámetros con los umbrales adecuados.
  - Analice los datos del generador de perfiles para identificar oportunidades de optimización
- CloudWatch Eventos: configure la supervisión basada en eventos para los eventos del clúster de Amazon DocumentDB.
  - Configure las notificaciones para los eventos de copia de seguridad, los períodos de mantenimiento y las conmutaciones por error.
  - Intégrelo con Amazon SNS para recibir alertas y respuestas automatizadas AWS Lambda .
- Registro de auditoría: planifique la configuración del registro de auditoría para rastrear la actividad de los usuarios y los eventos relevantes para la seguridad.
- Supervisión mejorada: habilite una supervisión mejorada para obtener métricas granulares a nivel del sistema operativo en intervalos de 1 segundo.

Migración de índices

La migración de MongoDB a Amazon DocumentDB implica transferir no solo datos, sino también índices para mantener el rendimiento de las consultas y optimizar las operaciones de la base de datos. En esta sección se describe el step-by-step proceso detallado para migrar índices de MongoDB a Amazon DocumentDB y, al mismo tiempo, garantizar la compatibilidad y la eficacia.

Uso de la herramienta de indexación de Amazon DocumentDB

Clonación de la herramienta de indexación

```
git clone https://github.com/aws-samples/amazon-documentdb-tools.git
cd amazon-documentdb-tools/index-tool
```

```
pip install -r requirements.txt
```

Exportación de índices desde MongoDB (si se migra desde MongoDB)

```
python3 migrationtools/documentdb_index_tool.py --dump-indexes --dir
 mongodb_index_export --uri
'mongodb://localhost:27017'
```

Exportación de índices desde Amazon DocumentDB (si se migra desde Amazon DocumentDB)

```
python3 migrationtools/documentdb_index_tool.py --dump-indexes --dir docdb_index_export
 --uri
'mongodb://user:password@mydocdb.cluster-cdtjj00yfi95.eu-west-
2.docdb.amazonaws.com:27017/?tls=true&tlsCAFile=rds-combined-ca-
bundle.pem&replicaSet=rs0&retryWrites=false'
```

Índices de importación

```
python3 migrationtools/documentdb_index_tool.py --restore-indexes --skip-incompatible
 --dir
mongodb_index_export --uri 'mongodb://user:password@mydocdb.cluster-cdtjj00yfi95.eu-
west-
2.docdb.amazonaws.com:27017/?tls=true&tlsCAFile=rds-combined-ca-
bundle.pem&replicaSet=rs0&retryWrites=false'
```

Verificación de índices

```
python3 migrationtools/documentdb_index_tool.py --show-issues --dir
 mongodb_index_export
```

Migración de usuario

La migración de usuarios de MongoDB a Amazon DocumentDB es esencial para mantener el control de acceso, la autenticación y la seguridad de la base de datos. En esta sección se describen los pasos detallados para migrar correctamente los usuarios de MongoDB y, al mismo tiempo, conservar sus roles y permisos mediante la herramienta de exportación de usuarios de Amazon DocumentDB.

Uso de la herramienta de exportación de usuarios de Amazon DocumentDB

`Export Users tool`Exporta los usuarios y las funciones de MongoDB o Amazon DocumentDB JavaScript a archivos, que luego se pueden usar para volver a crearlos en otro clúster.

Requisitos previos

```
# Clone the repository
git clone https://github.com/awslabs/amazon-documentdb-tools.git
cd amazon-documentdb-tools/migration/export-users
```

```
# Install required dependencies
pip install pymongo
```

Paso 1: exportar usuarios y roles

```
# Export users and roles to JavaScript files
python3 docdbExportUsers.py \
--users-file mongodb-users.js \
--roles-file mongodb-roles.js \
--uri "mongodb://admin:password@source-host:27017/"
```

Paso 2: editar el archivo de usuarios

```
// Example of how to update the users.js file
// Find each user creation statement and add the password
db.getSiblingDB("admin").createUser({
user: "appuser",
// Add password here
pwd: "newpassword",
roles: [
{ role: "readWrite", db: "mydb" }
]
})
```

Paso 3: restaurar roles personalizados en Amazon DocumentDB

```
# Import roles first
mongo --ssl \
--host target-host:27017 \
--sslCAFile rds-combined-ca-bundle.pem \
--username admin \
--password password \
mongodb-roles.js
```

Paso 4: restaurar usuarios en Amazon DocumentDB

```
# Import users after roles are created
mongo --ssl \
--host target-host:27017 \
--sslCAFile rds-combined-ca-bundle.pem \
--username admin \
--password password \
mongodb-users.js
```

Notas importantes

- Las contraseñas no se exportan por motivos de seguridad y deben añadirse manualmente al archivo users.js.
- Los roles se deben importar antes que los usuarios para garantizar una asignación de roles adecuada.
- La herramienta genera JavaScript archivos que se pueden ejecutar directamente con el shell mongo.
- Los roles personalizados y sus privilegios se conservan durante la migración.
- Este enfoque permite revisar y modificar los permisos de los usuarios antes de importarlos.

Este método proporciona un enfoque seguro y flexible para migrar usuarios y roles de MongoDB a Amazon DocumentDB y, al mismo tiempo, permite restablecer las contraseñas durante el proceso de migración.

Migración de datos

Temas

- Migración en línea
- Migración sin conexión
- Requisitos previos
- Preparación de un clúster de Amazon DocumentDB
- Realización de volcado de datos (mongodump)
- Transferencia de archivos de volcado al entorno de restauración
- Restauración de datos en Amazon DocumentDB (mongorestore)

Migración en línea

En esta sección se proporcionan pasos detallados para realizar una migración en línea de MongoDB a Amazon DocumentDB para permitir un tiempo de inactividad mínimo y AWS DMS una replicación continua. Para empezar, debe configurar un clúster de Amazon DocumentDB como destino y asegurarse de que su instancia de MongoDB esté correctamente configurada como el origen, lo que normalmente requiere el modo de conjunto de réplicas para la captura de datos de cambios. A continuación, debe crear una instancia de replicación de DMS y definir los puntos de conexión de origen y destino con los detalles de conexión necesarios. Tras validar los puntos de conexión, debe configurar e iniciar una tarea de migración que puede incluir la carga completa de los datos, la replicación continua o ambas.

Configuración del destino (Amazon DocumentDB)

> **Note**
>
> Si ya ha aprovisionado un clúster de Amazon DocumentDB al que migrar, puede omitir este paso.

Cree un grupo de parámetros personalizado

Consulte los AWS CLI procedimientos Consola de administración de AWS o enCreación de grupos de parámetros de clúster de Amazon DocumentDB.

Create an Amazon DocumentDB cluster (Crear un clúster de Amazon DocumentDB)

> **Note**
>
> Si bien en esta guía hay otros procedimientos para crear un clúster de Amazon DocumentDB, los pasos de esta sección se aplican específicamente a la tarea de migrar grandes cantidades de datos a un nuevo clúster.

1. Inicie sesión en y abra la Consola de administración de AWS consola de Amazon DocumentDB en https://console.aws.amazon.com /docdb.
2. En el panel de navegación, seleccione Clusters (Clústeres).

   > **Tip**
   >
   > Si no ve el panel de navegación del lado izquierdo de la pantalla, seleccione el icono de menú
   > (≡)
   > en la esquina superior izquierda de la página.

3. En la consola de administración de Amazon DocumentDB, en Clústeres, elija Crear.
4. En la página Crear clúster de Amazon DocumentDB, en la sección Tipo de clúster, elija Clúster basado en instancias (esta es la opción predeterminada).
5. En la sección Configuración de clúster:

   - En el campo Identificador del clúster, ingrese un nombre único, como **`mydocdbcluster`**. Tenga en cuenta que la consola cambiará todos los nombres de los clústeres a minúsculas independientemente de cómo se ingresen.
   - En Versión del motor, elija 5.0.0.

6. En la sección Configuración del almacenamiento en clúster, deje la opción Amazon DocumentDB estándar como se encuentra (es la opción predeterminada).
7. Sección de Configuración de instancias:

   - En Clase de instancia de base de datos, elija Clases optimizadas para memoria (incluidas las clases r), que es la opción predeterminada.
   - En Clase de instancia, elija una clase de instancia en función de la carga de trabajo. Por ejemplo:
     - db.r6g.large: para cargas de trabajo más pequeñas

- db.r6g.4xlarge: para cargas de trabajo más grandes

  Como práctica recomendada, sugerimos elegir una instancia del mayor tamaño posible para obtener el mejor rendimiento a carga completa y reducirla verticalmente una vez finalizada la migración.

- En Número de instancias, elija 1 instancia. La elección de una instancia ayuda a minimizar los costos. Recomendamos que escale a tres instancias para una alta disponibilidad después de que se complete la migración a carga completa.

8. En la sección Autenticación, ingrese un nombre de usuario para el usuario principal y, a continuación, elija Autoadministrado. Ingrese una contraseña y, a continuación, confírmela.
9. En la sección Configuración de red, elija una VPC y un grupo de subredes y, a continuación, configure el grupo de seguridad de la VPC. Actualice las reglas de entrada para asegurarse de que su grupo de seguridad de Amazon DocumentDB permita la conexión entrante desde el grupo de seguridad de la instancia de DMS.
10. En la ncryption-at-rest sección E, habilite el cifrado (recomendado) y elija o introduzca una clave KMS.
11. En la sección Copia de seguridad, establezca el período de retención de copia de seguridad (1-35 días).
12. Revise la configuración y elija Crear clúster.

    El tiempo de implementación suele tardar entre 10 y 15 minutos.

Configurar el origen

Tanto MongoDB como Amazon DocumentDB pueden servir como orígenes de migración, según la situación:

- MongoDB como fuente: común cuando se migra de un MongoDB local o autogestionado a Amazon DocumentDB u otros servicios de base de datos. AWS Requiere ejecutarse en modo conjunto de réplicas con un oplog del tamaño adecuado (asegúrese de que tenga el tamaño adecuado para contener todas las operaciones durante la carga completa) para permitir la captura de datos de cambios durante la migración.
- Amazon DocumentDB como origen: normalmente se utiliza para la replicación entre regiones, las actualizaciones de versiones o la migración a otros servicios de bases de datos, como MongoDB Atlas. Se requiere Habilitación de flujos de cambios mediante la configuración del parámetro `change_stream_log_retention_duration` en el grupo de parámetros del clúster para

capturar los cambios en curso durante la migración. Asegúrese de que la configuración de la `change_stream_log_retention_duration` sea lo suficientemente prolongada como para cubrir el tiempo necesario para concluir la carga completa.

Antes de iniciar la migración, configure la fuente para permitir el acceso. AWS DMS

Cree un usuario de MongoDB con los permisos adecuados:

```
db.createUser({
user: "dmsUser",
pwd: "yourSecurePassword",
roles: [{ role: "readAnyDatabase", db: "admin" }]
})
```

Configure la red y la autenticación.

Cuando configure la conectividad de red para la migración de MongoDB a DMS:

EC2-fuente MongoDB alojada

- Modifique el grupo EC2 de seguridad para permitir el tráfico entrante desde el grupo de seguridad de la instancia de replicación del DMS.
- Agregue una regla para el puerto TCP 27017 (o su puerto MongoDB personalizado).
- Utilice el identificador del grupo de seguridad de la instancia de replicación de DMS como origen para un control de acceso preciso.
- Asegúrese de que la subred de la EC2 instancia tenga una ruta a la subred de la instancia de replicación del DMS.

MongoDB en las instalaciones como origen

- Configure su firewall para permitir las conexiones entrantes desde las direcciones IP públicas de la instancia de replicación de DMS.
- Si utilizas Direct Connect una VPN, asegúrate de que se enrute correctamente entre la red y la VPC que contiene la instancia de DMS.
- Pruebe la conectividad mediante comandos telnet o nc desde la subred de DMS a su servidor MongoDB.

MongoDB Atlas como origen

- Agregue las direcciones IP de una instancia de replicación de DMS a la lista de IP permitidas de MongoDB Atlas.
- Configure el emparejamiento de VPC entre VPC y AWS MongoDB Atlas VPC si Atlas se está ejecutando. AWS
- Configúrelo AWS PrivateLink para la conectividad privada (nivel empresarial), si se ejecuta en otro proveedor de nube.
- Cree un usuario dedicado con read/write los permisos adecuados.
- Utilice una cadena de conexión de MongoDB Atlas con el modo SSL establecido en «verify-full».
- Asegúrese de que el tamaño del oplog sea suficiente para la duración de la migración.

Amazon DocumentDB como origen

Configure el grupo de seguridad de Amazon DocumentDB de origen para permitir el tráfico entrante desde el grupo de seguridad de la instancia de replicación de DMS.

Creación de una instancia de replicación de DMS

Recomendamos utilizar DMS Buddy para aprovisionar su infraestructura de DMS, ya que crea una infraestructura de migración óptima con una configuración de DMS y tamaños de instancia óptimos.

Si prefiere realizar la configuración manualmente, siga estos pasos:

1. Abra la consola AWS DMS y elija Crear instancia de replicación.
2. Introduzca los detalles de la instancia de replicación:
    - Nombre de la instancia: elija un nombre único.
    - Clase de instancia: selecciónela en función de la carga de trabajo. Ejemplo: dms.r5.large (cargas de trabajo pequeñas), dms.r5.4xlarge (cargas de trabajo grandes).
    - Versión del motor: 3.5.4
    - Almacenamiento asignado: el valor predeterminado es 100 GB (puede aumentarse si es necesario). Esto viene determinado por el tamaño del documento updates/second y la duración de la carga completa.
    - Implementación multi-AZ: se habilita para una alta disponibilidad, si es necesario.
    - Elija la misma VPC que Amazon DocumentDB.

- Asegúrese de que los grupos de seguridad permitan el tráfico entrante desde el origen y Amazon DocumentDB.

3. Haga clic en Crear instancia de replicación y espere a que el estado esté disponible.

Creación de puntos de conexión de DMS

Creación de un punto de conexión de origen

Si se toma MongoDB como origen

1. En la consola de DMS, en el panel de navegación, elija Migrar o replicar y, a continuación, elija Puntos de conexión.
2. Seleccione Crear punto de conexión.
3. En la página Crear punto de conexión, elija Punto de conexión de origen.
4. En la sección Configuración de punto de conexión:

   - Introduzca un Identificador de punto de conexión único y significativo (por ejemplo, «mongodb-source»).
   - Elija MongoDB como motor de origen.
   - Para acceder a la base de datos de puntos de conexión, elija Proporcionar información de acceso manualmente.
   - En Nombre del servidor, introduzca su*MongoDB server DNS name/IP address*.
   - En Puerto, introduzca 27017 (puerto MongoDB predeterminado).
   - En Modo de autenticación, elija el modo adecuado para su aplicación (contraseña/SSL) (el predeterminado es el administrador de secretos).
   - Si el Modo de autenticación es Contraseña, proporcione:
     - Nombre de usuario y Contraseña: escriba las credenciales de MongoDB.
     - Nombre de base de datos: el nombre de la base de datos de origen.
     - Mecanismo de autenticación: SCRAM-SHA-1 (predeterminado) o mecanismo apropiado.
5. En Modo de metadatos, deje la configuración predeterminada del documento.
6. Atributos de conexión adicionales:

   - authSource=admin (si la base de datos de autenticación es diferente).
   - ReplicaSet=< your-replica-set-name > (obligatorio para los CDC)

Si se toma Amazon DocumentDB como origen

1. En la consola de DMS, en el panel de navegación, elija Migrar o replicar y, a continuación, elija Puntos de conexión.
2. Seleccione Crear punto de conexión.
3. En la página Crear punto de conexión, elija Punto de conexión de origen.
4. En la sección Configuración de punto de conexión:
   - Introduzca un Identificador de punto de conexión único y significativo (por ejemplo, «docdb-source»).
   - Elija Amazon DocumentDB como motor de origen.
   - Para acceder a la base de datos de puntos de conexión, elija Proporcionar información de acceso manualmente.
   - En el nombre del servidor, introduzca su. *source Amazon DocumentDB cluster endpoint*
   - En Puerto ingrese 27017 (puerto predeterminado de Amazon DocumentDB).
   - En Modo SSL, elija verify-full (recomendado para Amazon DocumentDB).
   - En certificado CA, elija el certificado CA de Amazon RDS.
   - En Modo de autenticación, elija el modo adecuado para su aplicación (contraseña/SSL) (el predeterminado es el administrador de secretos).
   - Si el Modo de autenticación es Contraseña, proporcione:
     - Nombre de usuario y contraseña: introduzca las credenciales de Amazon DocumentDB.
     - Nombre de base de datos: el nombre de la base de datos de origen.
     - Mecanismo de autenticación: SCRAM-SHA-1 (predeterminado) o mecanismo apropiado.
5. En Modo de metadatos, deje la configuración predeterminada del documento.

Creación de un punto de conexión de destino (Amazon DocumentDB)

1. En la consola de DMS, en el panel de navegación, elija Migrar o replicar y, a continuación, elija Puntos de conexión.
2. Seleccione Crear punto de conexión.
3. En la página Crear punto de conexión, elija Punto de conexión de destino.
4. En la sección Configuración de punto de conexión:

- Introduzca un Identificador de punto de conexión único y significativo (por ejemplo, «docdb-target»).
- Elija Amazon DocumentDB como Motor de destino.
- En Acceder a la base de datos de puntos de conexión, elija el método que desee utilizar para autenticar el acceso a la base de datos:
  - Si elige Secrets Manager de AWS , elija el secreto en el que guarda sus credenciales de Amazon DocumentDB en el campo Secreto.
  - Si elige Proporcionar información de acceso manualmente:
    - En Nombre del servidor, introduzca su*target Amazon DocumentDB cluster endpoint*.
    - En Puerto ingrese 27017 (puerto predeterminado de Amazon DocumentDB).
    - En Modo SSL, elija verify-full (recomendado para Amazon DocumentDB).
    - En certificado CA, descargue y especifique el paquete de certificados CA para la verificación de SSL.
    - En Modo de autenticación, elija el modo adecuado para su aplicación (contraseña/SSL) (el predeterminado es el administrador de secretos).
    - Si el Modo de autenticación es Contraseña, proporcione:
      - Nombre de usuario y contraseña: introduzca las credenciales de Amazon DocumentDB.
      - Nombre de base de datos: el nombre de la base de datos de origen.
      - Mecanismo de autenticación: SCRAM-SHA-1 (predeterminado) o mecanismo apropiado.

5. En Modo de metadatos, deje la configuración predeterminada del documento.

Creación de una tarea de replicación

1. En la consola de DMS, en el panel de navegación, elija Migrar o replicar y, a continuación, elija Tareas.
2. Seleccione Crear tarea.
3. En la página Crear tarea, en la sección Configuración de tareas:
   - Introduzca un identificador de tarea único y significativo (por ejemplo, "mongodb-docdb-replication«).

- Elija el punto de conexión de origen que creó anteriormente en el menú desplegable de Punto de conexión de la base de datos de origen.
- Elija el punto de conexión de destino que creó anteriormente en el menú desplegable de Punto de conexión de la base de datos de destino.
- En Tipo de tarea, elija Migrar y replicar.

4. En la sección Configuración:

   - En el Modo de preparación de la tabla de destino, deje la configuración predeterminada.
   - En Detener la tarea después de que concluya la carga completa, deje la configuración predeterminada.
   - En Configuración de columnas de LOB, deje la configuración del Modo LOB limitado como está.
   - En Validación de datos, deje Desactivar, la configuración predeterminada.
   - Para los registros de tareas, marca la casilla Activar CloudWatch los registros.
   - En Aplicar optimización por lotes, deje la configuración predeterminada, es decir, desactivada (sin marcar).

5. Regrese a la parte superior de la sección Configuración de tareas. En el Modo de edición, seleccione Editor JSON y establezca los siguientes atributos:

```
{
  "TargetMetadata": {
    "ParallelApplyThreads": 5
  },
  "FullLoadSettings": {
    "MaxFullLoadSubTasks": 16
  }
}
```

6. En la sección Mapeos de tabla, añada una nueva regla de selección.

   - En Nombre del esquema, añada la base de datos de origen que quiere migrar. Utilice % para especificar bases de datos múltiples.
   - En Tabla del esquema, añada la colección de origen que quiere migrar. Utilice % para especificar colecciones múltiples.
   - En Acción, deje Incluir, la configuración predeterminada.

7. Para colecciones grandes (más de 100 GB), añada la Regla de configuración de tablas:

- En Nombre del esquema, añada la base de datos de origen que quiere migrar. Utilice % para especificar bases de datos múltiples.
- En Tabla del esquema, añada la colección de origen que quiere migrar. Utilice % para especificar colecciones múltiples.
- En Número de particiones, escriba 16 (debe ser menor que `MaxFullLoadSubTask`).

8. En la sección Evaluación previa a la migración, asegúrese de que esté desactivada.

Migración sin conexión

En esta sección se describe el proceso para realizar una migración sin conexión desde una instancia de MongoDB autogestionada a Amazon DocumentDB mediante herramientas nativas de MongoDB: `mongodump` y `mongorestore`.

Requisitos previos

Requisitos de MongoDB como origen

- Acceda a la instancia de MongoDB de origen con los permisos adecuados.
- Instale `mongodump` si es necesario (se instala durante una instalación de MongoDB).
- Asegúrese de que haya suficiente espacio en disco para los archivos de volcado.

Requisitos de Amazon DocumentDB como destino

- Asegúrese de tener aprovisionado un clúster de Amazon DocumentDB.
- Asegúrese de que haya una EC2 instancia en la misma VPC que Amazon DocumentDB para facilitar la migración.
- La conectividad de red debe estar disponible entre el entorno de origen y Amazon DocumentDB.
- mongorestore debe estar instalado en la instancia de migración. EC2
- Se deben configurar los permisos de IAM adecuados para acceder a Amazon DocumentDB.

Requisitos generales

- AWS CLI debe configurarse (si se utilizan AWS servicios de almacenamiento intermedio)
- Debe haber un ancho de banda suficiente para la transferencia de datos.

- Se debe aprobar el tiempo de inactividad (si realiza una migración en vivo, considere otros enfoques).

Preparación de un clúster de Amazon DocumentDB

Creación de un clúster de Amazon DocumentDB en AWS:

- Asigne un tamaño de instancia en función de su carga de trabajo.
- Configure una VPC, subredes y grupos de seguridad.
- Habilite los parámetros necesarios mediante grupos de parámetros.

Realización de volcado de datos (mongodump)

Elija una de las siguientes opciones para crear un archivo de volcado:

- Opción 1: básica

```
mongodump --
uri="mongodb://<source_user>:<source_password>@<source_host>:<source_port>/
<database>" --
out=/path/to/dump
```

- Opción 2: mejor control y rendimiento

```
mongodump \
--uri="mongodb://<source_user>:<source_password>@<sourcehost>:<source_port>" \
--out=/path/to/dump \
--gzip \# Compress output
--numParallelCollections=4 \# Parallel collections dump
--ssl \# If using SSL
--authenticationDatabase=admin \ # If auth is required
--readPreference=secondaryPreferred # If replica set
```

- Opción 3: bases de datos de gran tamaño

```
mongodump \
--host=<source_host> \
--port=<source_port> \
--username=<source_user> \
--password=<source_password> \
```

```
--db=<specific_db> \# Only dump specific DB
--collection=<specific_collection> \ # Only dump specific collection
--query='{ "date": { "$gt": "2020-01-01" } }' \ # Filter documents
--archive=/path/to/archive.gz \# Single archive output
--gzip \
--ssl
```

Transferencia de archivos de volcado al entorno de restauración

Elija un método adecuado en función del tamaño del volcado:

- Pequeño: copia directamente a tu máquina de migración (EC2 instancia que creaste anteriormente):

```
scp -r /path/to/dump user@migration-machine:/path/to/restore
```

- Mediano: utilice Amazon S3 como almacenamiento intermedio:

```
aws s3 cp --recursive /path/to/dump s3://your-bucket/mongodb-dump/
```

- Grande: para bases de datos muy grandes, considere AWS DataSync la posibilidad de realizar una transferencia física.

Restauración de datos en Amazon DocumentDB (mongorestore)

Antes de iniciar el proceso de restauración, cree los índices en Amazon DocumentDB. Puede utilizar la herramienta de indexación de Amazon DocumentDB para exportar e importar índices.

Seleccione una de las siguientes opciones para restaurar los datos:

- Opción 1: restauración básica

```
mongorestore --uri="mongodb://<docdb_user>:<docdb_password>@<docdb_endpoint>:27017"
/path/to/dump
```

- Opción 2: mejor control y rendimiento

```
mongorestore \
--uri="mongodb://<docdb_user>:<docdb_password>@<docdb_endpoint>:27017" \
--ssl \
```

```
--sslCAFile=/path/to/rds-combined-ca-bundle.pem \ # DocumentDB CA cert
--gzip \# If dumped with gzip
--numParallelCollections=4 \# Parallel restoration
--numInsertionWorkersPerCollection=4 \# Parallel documents insertion
--noIndexRestore \# skip indexes as they are pre-created
/path/to/dump
```

- Opción 3: bases de datos grandes o controles específicos

```
mongorestore \
--host=<docdb_endpoint> \
--port=27017 \
--username=<docdb_user> \
--password=<docdb_password> \
--ssl \
--sslCAFile=/path/to/rds-combined-ca-bundle.pem \
--archive=/path/to/archive.gz \# If using archive format
--gzip \
--nsInclude="db1.*" \# Only restore specific namespaces
--nsExclude="db1.sensitive_data" \ # Exclude specific collections if needed
--noIndexRestore \# skip indexes as they are pre-created
--writeConcern="{w: 'majority'}" # Ensure write durability
```

Supervisión

En esta sección se proporciona un proceso de supervisión detallado para hacer un seguimiento del progreso, el rendimiento y el estado de una migración en curso:

De MongoDB a Amazon DocumentDB

o

De Amazon DocumentDB a Amazon DocumentDB

Los pasos de supervisión se aplican independientemente del método de migración (AWS DMS, mongodump/mongorestore u otras herramientas).

AWS DMS Supervisión de la migración (si corresponde)

Supervise las siguientes CloudWatch métricas clave:

Métricas de la fase de carga completa

- FullLoadThroughputBandwidthTarget— Ancho de banda de red (KB/segundo) a plena carga
- FullLoadThroughputRowsTarget— Número de cargas por rows/documents segundo
- FullLoadThroughputTablesTarget— Número de unidades tables/collections completadas por minuto
- FullLoadProgressPercent— Porcentaje de carga completa completada
- TablesLoaded— Número de cargadas tables/collections correctamente
- TablesLoading— Número de personas que se tables/collections están cargando actualmente
- TablesQueued— Número de personas en tables/collections espera de ser cargadas
- TablesErrored— Número de los tables/collections que no se pudieron cargar

Métricas de la fase de CDC

- CDCLatencyObjetivo: retraso (segundos) entre el cambio de fuente y la aplicación de destino
- CDCLatencyFuente: retraso (segundos) entre el cambio en la fuente y la lectura del DMS
- CDCThroughputRowsTarget— Se aplicaron filas por segundo durante la replicación en curso
- CDCThroughputBandwidthTarget— Ancho de banda de red (KB/segundo) durante la CDC
- CDCIncomingCambios: número de eventos de cambio recibidos de la fuente
- CDCChangesMemoryTarget— Memoria utilizada (MB) para almacenar los cambios en el lado de destino

Métricas de recursos

- CPUUtilization— Uso de CPU de la instancia de replicación
- FreeableMemory— Memoria disponible en la instancia de replicación
- FreeStorageSpace— Almacenamiento disponible en la instancia de replicación
- NetworkTransmitThroughput— Rendimiento de red para la instancia de replicación
- NetworkReceiveThroughput— Rendimiento de red para la instancia de replicación

Métricas de errores

- ErrorsCount— Número total de errores durante la migración
- TableErrorsCount— Número de errores específicos de la tabla
- RecordsErrorsCount— Número de errores específicos del registro

Cree CloudWatch alarmas para métricas críticas, como `CDCLatencyTarget` recibir notificaciones si `CPUUtilization` el rendimiento de la migración se deteriora.

Registros de DMS (registros) CloudWatch

1. Ve a la consola de Amazon CloudWatch Logs.
2. Busque y elija un elemento de su grupo de registro. Tendrá un aspecto similar a «dms-tasks –».
3. Busque flujos de registro que puedan contener información de error:
   - Flujos con la palabra «error» en el nombre
   - Transmisiones con nombres de tareas IDs o puntos finales
   - Los flujos de registro más recientes durante el tiempo de la migración
4. En estos flujos, busque palabras clave como:
   - «error» (error)
   - «exception» (excepción)
   - «failed» (fallo)
   - «warning» (advertencia)

Estado de la tarea de DMS (utilizando AWS CLI)

```
aws dms describe-replication-tasks --filters Name=replication-task id,Values=<task_id>
 --query
"ReplicationTasks[0].Status"
```

Flujo de estado previsto:

crear → listo → en ejecución → detener → detenido (o fallido)

Supervise usando **`docdb-dashboarder`**

La `docdb-dashboarder` herramienta proporciona una supervisión integral de los clústeres de Amazon DocumentDB mediante la generación automática de CloudWatch cuadros de mando con las métricas de rendimiento esenciales. Estos paneles muestran métricas críticas a nivel de clúster (retraso de réplica, contadores de operaciones), métricas a nivel de instancia (CPU, memoria, conexiones) y métricas de almacenamiento (uso del volumen, almacenamiento de copias de seguridad). Para las situaciones de migración, la herramienta ofrece paneles especializados

que rastrean el progreso de la migración con métricas como el retraso en la replicación de la CDC y las tasas de operación. Los paneles pueden monitorear varios clústeres simultáneamente e incluyen soporte para NVMe instancias respaldadas. Si visualiza estas métricas, los equipos pueden identificar de forma proactiva los cuellos de botella en el rendimiento, optimizar la asignación de recursos y garantizar el buen funcionamiento de sus implementaciones de Amazon DocumentDB. La herramienta elimina la necesidad de crear un panel manual y, al mismo tiempo, proporciona una supervisión uniforme en todos los entornos. Para obtener instrucciones de configuración y opciones de configuración avanzadas, consulte el repositorio de herramientas Amazon DocumentDB Dashboarder. GitHub

Validación

Temas

- Lista de comprobación de validación
- Validación de esquemas e índices
- Muestreo de datos y validación a nivel de campo
- Validación mediante herramienta DataDiffer

En esta sección se proporciona un proceso de validación detallado para garantizar la coherencia de datos, la integridad y la compatibilidad de las aplicaciones tras la migración:

De MongoDB a Amazon DocumentDB

o

De Amazon DocumentDB a Amazon DocumentDB

Los pasos de validación se aplican independientemente del método de migración (AWS DMS, mongodump/mongorestore u otras herramientas).

Lista de comprobación de validación

Compruebe que el número de documentos de cada colección coincide con el de origen y el de destino:

MongoDB como origen

```
mongo --host <source_host> --port <port> --username <user> -- password <password> --
eval
```

```
"db.<collection>.count()"
```

Amazon DocumentDB como destino

```
mongo --host <target_host> --port <port> --username <user> -- password <password> --
eval
"db.<collection>.count()"
```

Validación de esquemas e índices

Asegúrese de que:

- Todas las colecciones existen en el destino.
- Los índices se replican correctamente.
- Las definiciones de esquema (si se imponen) son idénticas.

Comprobación de colecciones (origen frente a destino)

```
mongo --host <source_host> --eval "show collections"
mongo --host <target_host> --ssl --eval "show collections"
```

Comprobación de índices (origen frente a destino)

```
mongo --host <source_host> --eval" db.<collection>.getIndexes()"
mongo --host <target_host> --ssl –eval" db.<collection>.getIndexes()"
```

Compare la lista de colecciones para asegurarse de que no haya colecciones faltantes ni adicionales.

Verifique los índices. Para ello, compruebe los nombres de los índices, las definiciones clave, las restricciones únicas y los índices TTL (si los hubiera).

Comprobación de reglas de validación de esquemas (si usa la validación de esquemas en MongoDB)

```
mongo --host <source_host> --eval" db.getCollectionInfos({name: '<collection>'})
[0].options.validator"
   mongo --host <target_host> --ssl –eval" db.getCollectionInfos({name:
 '<collection>'})[0].options.validator"
```

Muestreo de datos y validación a nivel de campo

Puede muestrear documentos de forma aleatoria y comparar campos entre el origen y el destino.

Muestreo manual

Obtenga cinco documentos aleatorios (origen):

```
mongo --host <source_host> --eval "db.<collection>.aggregate([{ \$sample: { size:
 5 } }])"
```

Obtenga el mismo documento IDs (destino):

```
mongo --host <target_host> --ssl -eval "db.<collection>.find({ _id: { \$in:
 [<list_of_ids>] } })"
```

Muestreo automático

```
import pymongo
# Connect to source and target
source_client = pymongo.MongoClient("<source_uri>")
target_client = pymongo.MongoClient("<target_uri>", ssl=True)
source_db = source_client["<db_name>"]
target_db = target_client["<db_name>"]
# Compare 100 random documents
for doc in source_db.<collection>.aggregate([{ "$sample":
{ "size": 100 } }]):
target_doc = target_db.<collection>.find_one({ "_id":
doc["_id"] })
if target_doc != doc:
print(f"# Mismatch in _id: {doc['_id']}")
else:
print(f"# Match: {doc['_id']}")
```

Validación mediante herramienta DataDiffer

La DataDiffer herramienta proporciona una forma fiable de comparar los datos entre las bases de datos de origen y destino.

Requisitos previos

Se deben cumplir los siguientes requisitos previos antes de instalar la DataDiffer herramienta:

- Python 3.7+
- PyMongo biblioteca
- Conectividad de red con los clústeres de MongoDB de origen y de Amazon DocumentDB de destino

Instalación y configuración

Clona el repositorio y navega hasta el DataDiffer directorio

```
git clone https://github.com/awslabs/amazon-documentdb-tools.git
cd amazon-documentdb-tools/migration/data-differ
```

Instale las dependencias requeridas.

```
pip install -r requirements.txt
```

Ejecución de validación de datos

Cree un archivo de configuración (por ejemplo, config.json) con los detalles de la conexión.

```
{
"source": {
"uri": "mongodb://username:password@source-mongodb-
host:27017/?replicaSet=rs0",
"db": "your_database",
"collection": "your_collection"
},
"target": {
"uri": "mongodb://username:password@target-docdb-
cluster.region.docdb.amazonaws.com:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0",
"db": "your_database",
"collection": "your_collection"
},
"options": {
"batch_size": 1000,
"threads": 4,
"sample_size": 0,
"verbose": true
}
}
```

Ejecute la DataDiffer herramienta

```
python differ.py --config config.json
```

En el caso de colecciones grandes, utilice el muestreo para validar un subconjunto de datos.

```
python differ.py --config config.json --sample-size 10000
```

Para validar varias colecciones, cree archivos de configuración independientes o utilice el modo por lotes

```
python differ.py --batch-config batch_config.json
```

Interpretación de los resultados

El resultado que mostrará la herramienta incluirá lo siguiente:

- Documentos totales de origen y destino
- Número de documentos coincidentes
- Número de documentos faltantes
- Número de documentos con diferencias
- Informe detallado de las diferencias (si las hubiera)

Prácticas recomendadas

Las siguientes son las prácticas recomendadas a la hora de utilizar la DataDiffer herramienta:

- Ejecute por fases: primero valide los recuentos de documentos, luego tome muestras de los documentos clave y, finalmente, ejecute una comparación completa, si es necesario.
- Compruebe si hay diferencias en los esquemas: Amazon DocumentDB tiene algunas limitaciones en comparación con MongoDB. La herramienta destacará los tipos o las estructuras de datos incompatibles.
- Valide durante los períodos de inactividad: ejecute la validación cuando las operaciones de escritura sean mínimas para garantizar la coherencia.
- Supervise el uso de los recursos: el proceso de comparación puede consumir muchos recursos. Ajuste el tamaño del lote y el número de subprocesos en consecuencia.

- Valide los índices: tras la validación de los datos, asegúrese de que se hayan creado todos los índices necesarios en el clúster de Amazon DocumentDB de destino.
- Resultados de la validación de documentos: mantenga un registro de los resultados de la validación de cada colección como parte de la documentación de migración.

Migración desde Couchbase Server

Temas

- Introducción
- Comparación con Amazon DocumentDB
- Discovery
- Planificación
- Migración
- Validación

Introducción

Esta guía presenta los puntos clave que se deben tener en cuenta al migrar de Couchbase Server a Amazon DocumentDB. Explica las consideraciones para las fases de descubrimiento, planificación, ejecución y validación de la migración. También explica cómo realizar migraciones en línea y fuera de línea.

Comparación con Amazon DocumentDB

	Servidor Couchbase	Amazon DocumentDB
Organización de datos	En las versiones 7.0 y posteriores, los datos se organizan en grupos, ámbitos y colecciones. En versiones anteriores, los datos se organizaban en cubos.	Los datos se organizan en bases de datos y colecciones.
Compatibilidad	Los hay distintos APIs para cada servicio (por ejemplo, datos, índices, búsquedas, etc.). Las	Amazon DocumentDB es compatible con la API de MongoDB.

	Servidor Couchbase	Amazon DocumentDB
	búsquedas secundarias utilizan SQL++ (antes conocido como N1QL), un lenguaje de consulta basado en el SQL estándar de ANSI, por lo que muchos desarroll adores lo conocen bien.	
Arquitectura	El almacenamiento está adjunto a cada instancia del clúster. No se puede escalar la computaci ón de forma independiente del almacenamiento.	Amazon DocumentDB está diseñado para la nube y para evitar las limitaciones de las arquitecturas de bases de datos tradicionales. Las capas de procesamiento y almacenam iento están separadas en Amazon DocumentDB y la capa de procesamiento se puede escalar independientemente del almacenamiento.
Añada capacidad de lectura a pedido	Los clústeres se pueden escalar agregando instancias. Como el almacenamiento está conectado a la instancia en la que se ejecuta el servicio, el tiempo que tarda en ampliarse depende de la cantidad de datos que deban trasladarse a la nueva instancia o reequilibrarse.	Puede lograr el escalado de lectura para su clúster de Amazon DocumentDB creando hasta 15 réplicas de Amazon DocumentD B en el clúster. No hay ningún impacto en la capa de almacenam iento.

	Servidor Couchbase	Amazon DocumentDB
Recupérese rápidamente de una falla en un nodo	Los clústeres tienen capacidades de conmutación por error automática, pero el tiempo necesario para que el clúster recupere toda su potencia depende de la cantidad de datos que se deban mover a la nueva instancia.	Amazon DocumentDB puede realizar la conmutación por error del principal normalmente en 30 segundos y restaurar el clúster a su estado completo en 8 a 10 minutos, independientemente de la cantidad de datos del clúster.
Amplíe el almacenamiento a medida que crecen los datos	Para el almacenamiento de clústeres autogestionados y IOs no lo escale automáticamente.	Almacene y IOs escale automáticamente en Amazon DocumentDB.
Backup de datos sin afectar el rendimiento	Las copias de seguridad las realiza el servicio de copias de seguridad y no están habilitadas de forma predeterminada. Como el almacenamiento y la computación no están separados, esto puede repercutir en el rendimiento.	Las copias de seguridad de Amazon DocumentDB están habilitadas de forma predeterminada y no se pueden desactivar. Las copias de seguridad las gestiona la capa de almacenamiento, por lo que no tienen ningún impacto en la capa de procesamiento. Amazon DocumentDB admite la restauración a partir de una instantánea de clúster y la restauración a un punto en el tiempo.

	Servidor Couchbase	Amazon DocumentDB
Durabilidad de los datos	Puede haber un máximo de 3 réplicas de datos en un clúster para un total de 4 copias. Cada instancia en la que se ejecute el servicio de datos tendrá copias activas y 1, 2 o 3 réplicas de los datos.	Amazon DocumentDB conserva 6 copias de los datos independientemente del número de instancias de cómputo que haya con un quórum de escritura de 4 y sigue siendo verdadero. Los clientes reciben un acuse de recibo cuando la capa de almacenamiento haya conservado 4 copias de los datos.
Coherencia	Se admite la coherencia inmediata de K/V las operaciones. El SDK de Couchbase dirige las K/V solicitudes a la instancia específica que contiene la copia activa de los datos, por lo que, una vez confirmada la actualización, el cliente tiene la garantía de leerla. Con el tiempo, la replicación de las actualizaciones en otros servicios (indexación, búsqueda, análisis, creación de eventos) es coherente.	Con el tiempo, las réplicas de Amazon DocumentDB son coherentes. Si se requieren lecturas de coherencia inmediata, el cliente puede leer desde la instancia principal.
Replicación	La replicación entre centros de datos (XDCR) proporciona una replicación de datos filtrada, activa-pasiva o activa-activa y activa, de datos en muchísimas topologías.	Los clústeres globales de Amazon DocumentDB proporcionan replicación activa-pasiva en topologías 1:muchos (hasta 10).

Discovery

La migración a Amazon DocumentDB requiere un conocimiento exhaustivo de la carga de trabajo de la base de datos existente. El descubrimiento de la carga de trabajo es el proceso de analizar la

configuración del clúster de Couchbase y las características operativas (conjunto de datos, índices y carga de trabajo) para garantizar una transición fluida con una interrupción mínima.

Configuración del clúster

Couchbase utiliza una arquitectura centrada en los servicios, en la que cada capacidad corresponde a un servicio. Ejecute el siguiente comando en su clúster de Couchbase para determinar qué servicios se están utilizando (consulte Obtener información sobre los nodos):

```
curl -v -u <administrator>:<password> \
  http://<ip-address-or-hostname>:<port>/pools/nodes | \
  jq '[.nodes[].services[]] | unique'
```

Código de salida de ejemplo:

```
[
  "backup",
  "cbas",
  "eventing",
  "fts",
  "index",
  "kv",
  "n1ql"
]
```

Los servicios de Couchbase incluyen lo siguiente:

Servicio de datos (kv)

El servicio de datos proporciona read/write acceso a los datos de la memoria y del disco.

Amazon DocumentDB admite K/V operaciones con datos JSON mediante la API de MongoDB.

Servicio de consultas (n1ql)

El servicio de consultas admite la consulta de datos JSON a través de SQL++.

Amazon DocumentDB admite la consulta de datos JSON mediante la API de MongoDB.

Servicio de indexación (índice)

El servicio de indexación crea y mantiene índices en los datos, lo que permite realizar consultas más rápidas.

Amazon DocumentDB admite un índice principal predeterminado y la creación de índices secundarios en datos JSON mediante la API de MongoDB.

Servicio de búsqueda (fts)

El servicio de búsqueda admite la creación de índices para la búsqueda de texto completo.

La función de búsqueda de texto completo nativa de Amazon DocumentDB le permite realizar búsquedas de texto en conjuntos de datos textuales de gran tamaño mediante índices de texto especiales mediante la API de MongoDB. Para los casos de uso de búsquedas avanzadas, la integración de Amazon DocumentDB Zero-ETL con Amazon OpenSearch Service proporciona capacidades de búsqueda avanzada, como la búsqueda difusa, la búsqueda cruzada entre colecciones y la búsqueda multilingüe, en los datos de Amazon DocumentDB.

Servicio de análisis (cbas)

El servicio de análisis permite analizar los datos de JSON prácticamente en tiempo real.

Amazon DocumentDB admite consultas ad hoc en datos JSON mediante la API de MongoDB. También puede ejecutar consultas complejas en sus datos JSON en Amazon DocumentDB mediante Apache Spark que se ejecuta en Amazon EMR.

Servicio de eventos (eventing)

El servicio de eventos ejecuta una lógica empresarial definida por el usuario en respuesta a los cambios en los datos.

Amazon DocumentDB automatiza las cargas de trabajo basadas en eventos mediante la invocación de AWS Lambda funciones cada vez que los datos cambian con el clúster de Amazon DocumentDB.

Servicio de backup (backup)

El servicio de respaldo programa copias de seguridad de datos completas e incrementales y fusiones de copias de seguridad de datos anteriores.

Amazon DocumentDB realiza copias de seguridad continuas de sus datos en Amazon S3 con un período de retención de 1 a 35 días para que pueda restaurarlos rápidamente en cualquier punto dentro del período de retención de la copia de seguridad. Amazon DocumentDB también toma instantáneas automáticas de los datos como parte de este proceso de copia de seguridad continua. También puede gestionar las copias de seguridad y la restauración de Amazon DocumentDB con. AWS Backup.

Características operativas

Utilice la herramienta de detección de Couchbase para obtener la siguiente información sobre su conjunto de datos, índices y carga de trabajo. Esta información le ayudará a dimensionar su clúster de Amazon DocumentDB.

Conjunto de datos

La herramienta recupera la siguiente información sobre el depósito, el alcance y la recopilación:

1. nombre del bucket
2. tipo de bucket
3. nombre del ámbito
4. nombre de la colección
5. tamaño total (bytes)
6. total de artículos
7. tamaño del artículo (bytes)

Índices

La herramienta recupera las siguientes estadísticas de índice y todas las definiciones de índice de todos los cubos. Tenga en cuenta que los índices principales están excluidos, ya que Amazon DocumentDB crea automáticamente un índice principal para cada colección.

1. nombre del bucket
2. nombre del ámbito
3. nombre de la colección
4. nombre del índice
5. tamaño del índice (bytes)

Carga de trabajo

La herramienta recupera las métricas de las K/V consultas de N1QL. K/V los valores de las métricas se recopilan a nivel de segmento y las métricas de SQL++ se recopilan a nivel de clúster.

Las opciones de la línea de comandos de la herramienta son las siguientes:

```
python3 discovery.py \
  --username <source cluster username> \
  --password <source cluster password> \
  --data_node <data node IP address or DNS name> \
  --admin_port <administration http REST port> \
  --kv_zoom <get bucket statistics for specified interval> \
  --tools_path <full path to Couchbase tools> \
  --index_metrics <gather index definitions and SQL++ metrics> \
  --indexer_port <indexer service http REST port> \
  --n1ql_start <start time for sampling> \
  --n1ql_step <sample interval over the sample period>
```

A continuación se muestra un comando de ejemplo:

```
python3 discovery.py \
  --username username \
  --password ******** \
  --data_node "http://10.0.0.1" \
  --admin_port 8091 \
  --kv_zoom week \
  --tools_path "/opt/couchbase/bin" \
  --index_metrics true \
  --indexer_port 9102 \
  --n1ql_start -60000 \
  --n1ql_step 1000
```

Los valores de las métricas K/V se basarán en muestras cada 10 minutos durante la semana pasada (consulte el método HTTP y el URI). Los valores métricos de SQL++ se basarán en muestras cada 1 segundo durante los últimos 60 segundos (consulte las etiquetas generales). El resultado del comando estará en los siguientes archivos:

collection-stats.csv: información sobre el depósito, el alcance y la recopilación

```
bucket,bucket_type,scope_name,collection_name,total_size,total_items,document_size
beer-sample,membase,_default,_default,2796956,7303,383
gamesim-sample,membase,_default,_default,114275,586,196
pillowfight,membase,_default,_default,1901907769,1000006,1902
travel-sample,membase,inventory,airport,547914,1968,279
travel-sample,membase,inventory,airline,117261,187,628
travel-sample,membase,inventory,route,13402503,24024,558
travel-sample,membase,inventory,landmark,3072746,4495,684
travel-sample,membase,inventory,hotel,4086989,917,4457
```

```
...
```

index-stats.csv: indexa nombres y tamaños

```
bucket,scope,collection,index-name,index-size
beer-sample,_default,_default,beer_primary,468144
gamesim-sample,_default,_default,gamesim_primary,87081
travel-sample,inventory,airline,def_inventory_airline_primary,198290
travel-sample,inventory,airport,def_inventory_airport_airportname,513805
travel-sample,inventory,airport,def_inventory_airport_city,487289
travel-sample,inventory,airport,def_inventory_airport_faa,526343
travel-sample,inventory,airport,def_inventory_airport_primary,287475
travel-sample,inventory,hotel,def_inventory_hotel_city,497125
...
```

kv-stats.csv: obtiene, establece y elimina las métricas de todos los grupos

```
bucket,gets,sets,deletes
beer-sample,0,0,0
gamesim-sample,0,0,0
pillowfight,369,521,194
travel-sample,0,0,0
```

n1ql-stats.csv: SQL++ selecciona, elimina e inserta métricas para el clúster

```
selects,deletes,inserts
0,132,87
```

indexes- .txt<bucket-name>: definiciones de índice de todos los índices del depósito. Tenga en cuenta que los índices principales están excluidos, ya que Amazon DocumentDB crea automáticamente un índice principal para cada colección.

```
CREATE INDEX `def_airportname` ON `travel-sample`(`airportname`)
CREATE INDEX `def_city` ON `travel-sample`(`city`)
CREATE INDEX `def_faa` ON `travel-sample`(`faa`)
CREATE INDEX `def_icao` ON `travel-sample`(`icao`)
CREATE INDEX `def_inventory_airport_city` ON `travel-
sample`.`inventory`.`airport`(`city`)
CREATE INDEX `def_inventory_airport_faa` ON `travel-
sample`.`inventory`.`airport`(`faa`)
```

```
CREATE INDEX `def_inventory_hotel_city` ON `travel-sample`.`inventory`.`hotel`(`city`)
CREATE INDEX `def_inventory_landmark_city` ON `travel-
sample`.`inventory`.`landmark`(`city`)
CREATE INDEX `def_sourceairport` ON `travel-sample`(`sourceairport`)
...
```

Planificación

En la fase de planificación, determinará los requisitos del clúster de Amazon DocumentDB y el mapeo de los depósitos, ámbitos y colecciones de Couchbase a las bases de datos y colecciones de Amazon DocumentDB.

Requisitos del clúster de Amazon DocumentDB

Utilice los datos recopilados en la fase de descubrimiento para dimensionar el clúster de Amazon DocumentDB. Consulte Dimensionamiento de instancias para obtener más información sobre el tamaño de su clúster de Amazon DocumentDB.

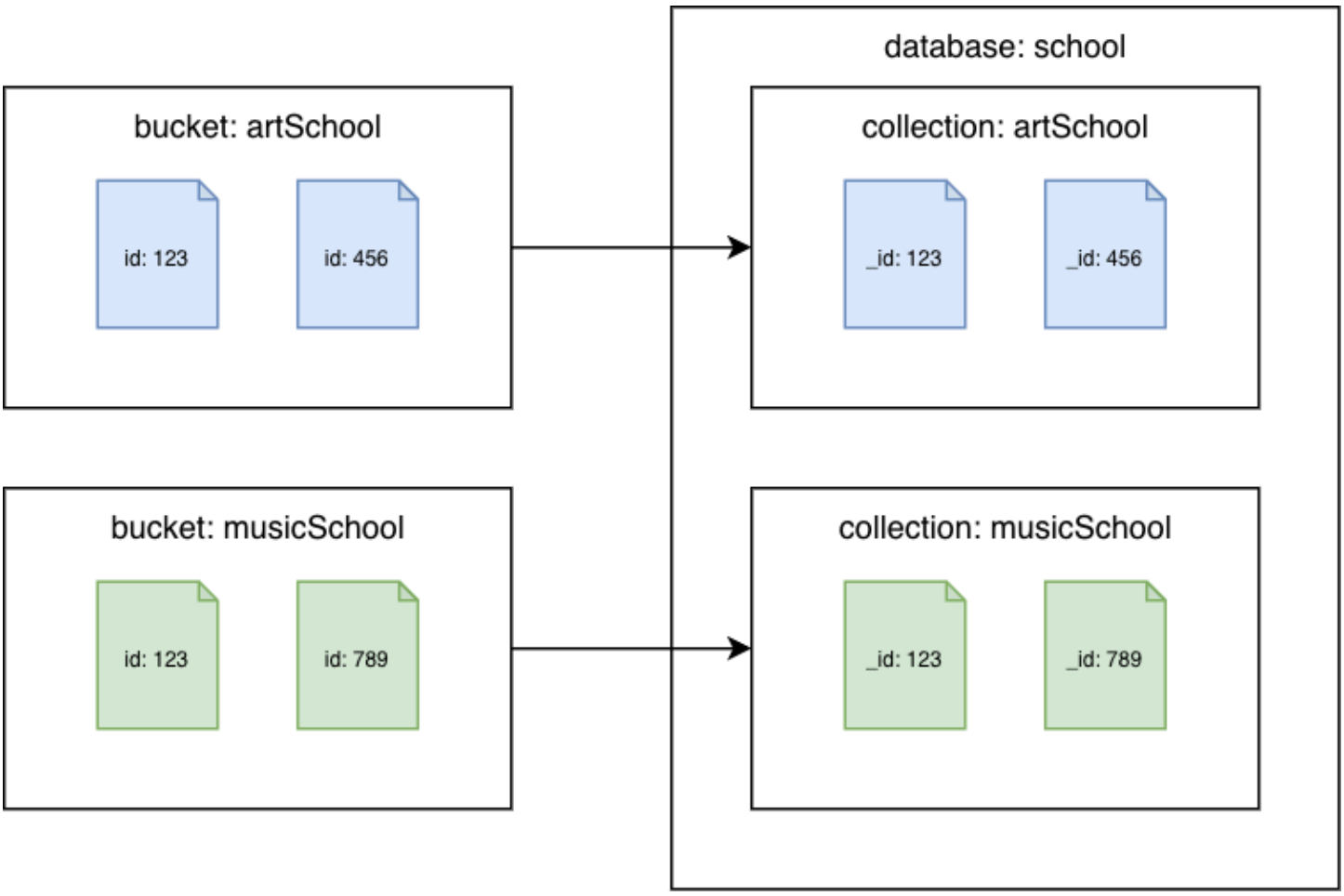
Asignación de depósitos, ámbitos y colecciones a bases de datos y colecciones

Determine las bases de datos y colecciones que existirán en sus clústeres de Amazon DocumentDB. Tenga en cuenta las siguientes opciones en función de cómo estén organizados los datos en su clúster de Couchbase. Estas no son las únicas opciones, pero proporcionan puntos de partida para que los tenga en cuenta.

Couchbase Server 6.x o anterior

Couchbase pasa a las colecciones de Amazon DocumentDB

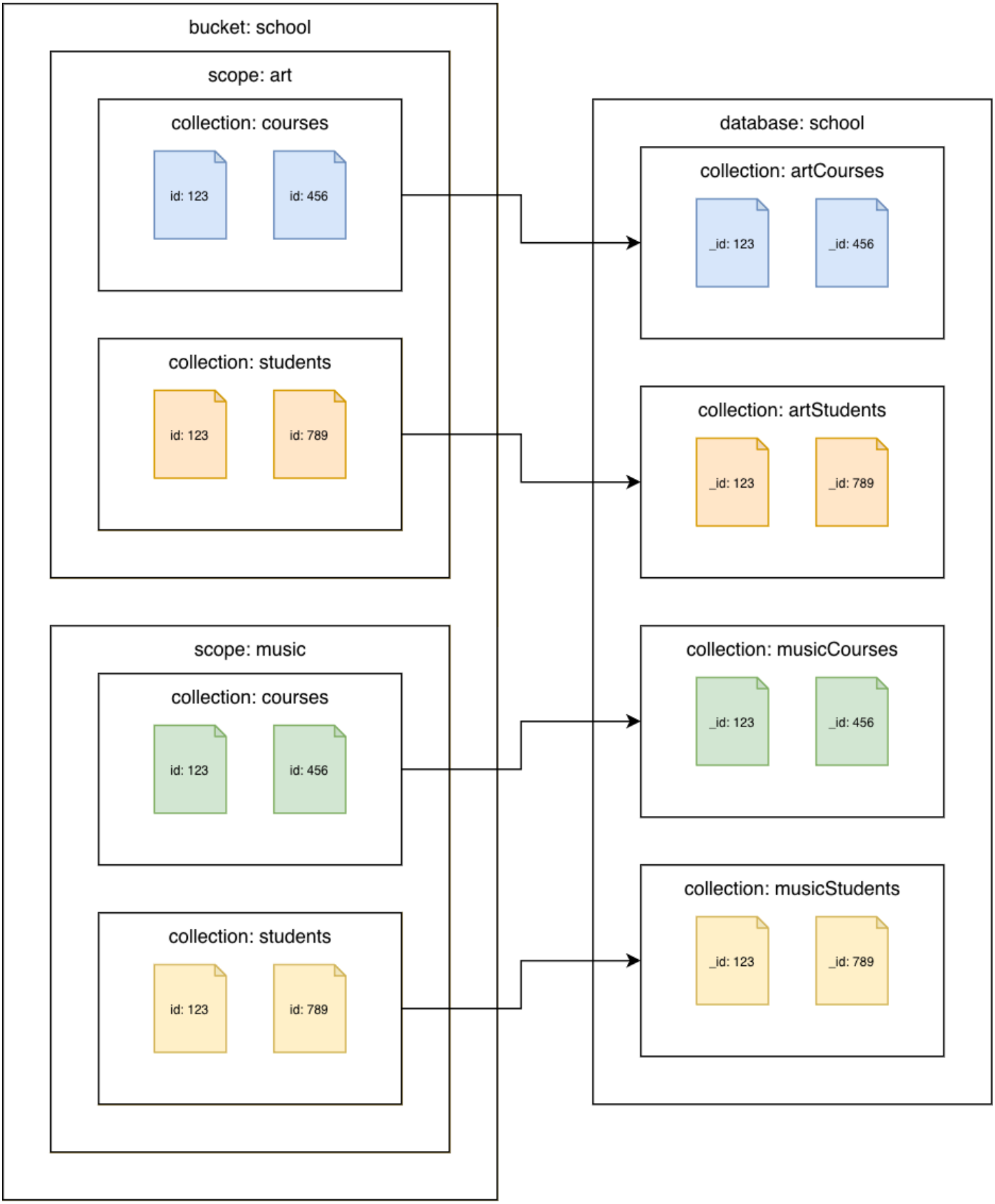
Migre cada depósito a una colección diferente de Amazon DocumentDB. En este escenario, el valor del documento de Couchbase se utilizará como `id` valor de Amazon `_id` DocumentDB.



Couchbase Server 7.0 o posterior

De las colecciones de Couchbase a las colecciones de Amazon DocumentDB

Migre cada colección a una colección diferente de Amazon DocumentDB. En este escenario, el valor del documento de Couchbase se utilizará como `id` valor de Amazon `_id` DocumentDB.


bucket: school
scope: art
collection: courses
id: 123
id: 456
collection: students
id: 123
id: 789
scope: music
collection: courses
id: 123
id: 456
collection: students
id: 123
id: 789
database: school
collection: artCourses
_id: 123
_id: 456
collection: artStudents
_id: 123
_id: 789
collection: musicCourses
_id: 123
_id: 456
collection: musicStudents
_id: 123
_id: 789

Migración

Migración de índices

La migración a Amazon DocumentDB implica transferir no solo datos, sino también índices para mantener el rendimiento de las consultas y optimizar las operaciones de la base de datos. En esta sección se describe el step-by-step proceso detallado para migrar índices a Amazon DocumentDB y, al mismo tiempo, garantizar la compatibilidad y la eficacia.

Utilice Amazon Q para convertir `CREATE INDEX` sentencias de SQL++ en comandos de Amazon `createIndex()` DocumentDB.

1. Cargue los archivos indexes-.txt <bucket name>creados por la herramienta de descubrimiento para Couchbase.
2. Introduzca el siguiente mensaje:

   ```
   Convert the Couchbase CREATE INDEX statements to Amazon DocumentDB
   createIndex commands
   ```

Amazon Q generará comandos de Amazon DocumentDB `createIndex()` equivalentes. Tenga en cuenta que es posible que tenga que actualizar los nombres de las colecciones en función de la forma en que haya asignado los buckets, los ámbitos y las colecciones de Couchbase a las colecciones de Amazon DocumentDB.

Por ejemplo:

indexes-beer-sample.txt

```
CREATE INDEX `beerType` ON `beer-sample`(`type`)
CREATE INDEX `code` ON `beer-sample`(`code`) WHERE (`type` = "brewery")
```

Ejemplo de salida de Amazon Q (extracto):

```
db.beerSample.createIndex(
  { "type": 1 },
  {
    "name": "beerType",
    "background": true
  }
)
```

```
db.beerSample.createIndex(
  { "code": 1 },
  {
    "name": "code",
    "background": true,
    "partialFilterExpression": { "type": "brewery" }
  }
)
```

Para obtener más información sobre los índices que Amazon Q no pueda convertir, consulte Administración de índices e índices de Amazon DocumentDB y propiedades de índices.

Refactoriza el código para usar MongoDB APIs

Los clientes usan Couchbase para conectarse al servidor Couchbase SDKs . Los clientes de Amazon DocumentDB utilizan los controladores MongoDB para conectarse a Amazon DocumentDB. Todos los idiomas compatibles con Couchbase también SDKs son compatibles con los controladores de MongoDB. Consulte Controladores MongoDB para obtener más información sobre el controlador para su idioma.

Como Couchbase Server y Amazon DocumentDB APIs son diferentes, tendrá que refactorizar el código para usar la MongoDB adecuada. APIs Puede usar Amazon Q para convertir las llamadas a la K/V API y las consultas de SQL++ en el MongoDB equivalente: APIs

1. Cargue los archivos de código fuente.
2. Introduzca el siguiente mensaje:

```
Convert the Couchbase API code to Amazon DocumentDB API code
```

Con el ejemplo de código Python de Hello Couchbase, Amazon Q genera lo siguiente (extracto):

```
from datetime import timedelta
from pymongo import MongoClient

# Connection parameters
database_name = "travel-sample"

# Connect to Amazon DocumentDB cluster
client = MongoClient('<Amazon DocumentDB connection string>')
```

```
# Get reference to database and collection
db = client['travel-sample']
airline_collection = db['airline']

# upsert document function
def upsert_document(doc):
    print("\nUpsert Result: ")
    try:
        # key will equal: "airline_8091"
        key = doc["type"] + "_" + str(doc["id"])
        doc['_id'] = key # Amazon DocumentDB uses _id as primary key
        result = airline_collection.update_one(
            {'_id': key},
            {'$set': doc},
            upsert=True
        )
        print(f"Modified count: {result.modified_count}")
    except Exception as e:
        print(e)

# get document function
def get_airline_by_key(key):
    print("\nGet Result: ")
    try:
        result = airline_collection.find_one({'_id': key})
        print(result)
    except Exception as e:
        print(e)

# query for document by callsign
def lookup_by_callsign(cs):
    print("\nLookup Result: ")
    try:
        result = airline_collection.find(
            {'callsign': cs},
            {'name': 1, '_id': 0}
        )
        for doc in result:
            print(doc['name'])
    except Exception as e:
        print(e)

# Test document
airline = {
```

```
    "type": "airline",
    "id": 8091,
    "callsign": "CBS",
    "iata": None,
    "icao": None,
    "name": "Couchbase Airways",
}

upsert_document(airline)
get_airline_by_key("airline_8091")
lookup_by_callsign("CBS")
```

Consulte Conexión mediante programación a Amazon DocumentDB para ver ejemplos de conexión a Amazon DocumentDB en Python, Node.js, PHP, Go, Java, C#/.NET, R y Ruby.

Seleccione el enfoque de migración

Al migrar datos a Amazon DocumentDB, hay dos opciones:

1. migración fuera de línea
2. migración en línea

Migración sin conexión

Considere la posibilidad de realizar una migración fuera de línea cuando:

- El tiempo de inactividad es aceptable: la migración sin conexión implica detener las operaciones de escritura en la base de datos de origen, exportar los datos y, a continuación, importarlos a Amazon DocumentDB. Este proceso provoca un tiempo de inactividad para la aplicación. Si su aplicación o carga de trabajo pueden tolerar este período de falta de disponibilidad, la migración sin conexión es una opción viable.
- Migrar conjuntos de datos más pequeños o realizar pruebas de concepto: en el caso de conjuntos de datos más pequeños, el tiempo necesario para el proceso de exportación e importación es relativamente corto, por lo que la migración sin conexión es un método rápido y sencillo. También es adecuado para el desarrollo, las pruebas y los proof-of-concept entornos en los que el tiempo de inactividad es menos crítico.
- La simplicidad es una prioridad: el método offline, que utiliza cbexport y mongoimport, suele ser el enfoque más sencillo para migrar datos. Evita las complejidades de la captura de datos de cambios (CDC) que implican los métodos de migración en línea.

- No es necesario replicar los cambios continuos: si la base de datos de origen no recibe cambios de forma activa durante la migración, o si esos cambios no son fundamentales para capturarlos y aplicarlos al destino durante el proceso de migración, es apropiado adoptar un enfoque fuera de línea.

Temas

- Couchbase Server 6.x o anterior
- Couchbase Server 7.0 o posterior

Couchbase Server 6.x o anterior

De Couchbase a la colección Amazon DocumentDB

Exporte los datos con cbexport json para crear un volcado JSON de todos los datos del depósito. Para `--format` esta opción, puede usar `lines` o. `list`

```
cbexport json \
  --cluster <source cluster endpoint> \
  --bucket <bucket name> \
  --format <lines | list> \
  --username <username> \
  --password <password> \
  --output export.json \
  --include-key _id
```

Importe los datos a una colección de Amazon DocumentDB mediante mongoimport con la opción adecuada para importar las líneas o la lista:

líneas:

```
mongoimport \
  --db <database> \
  --collection <collection> \
  --uri "<Amazon DocumentDB cluster connection string>" \
  --file export.json
```

lista:

```
mongoimport \
  --db <database> \
```

```
  --collection <collection> \
  --uri "<Amazon DocumentDB cluster connection string>" \
  --jsonArray \
  --file export.json
```

Couchbase Server 7.0 o posterior

Para realizar una migración sin conexión, utilice las herramientas cbexport y mongoimport:

Depósito de Couchbase con alcance y colección predeterminados

Exporte los datos con cbexport json para crear un volcado JSON de todas las colecciones del depósito. Para `--format` esta opción, puede usar `lines` o. `list`

```
cbexport json \
  --cluster <source cluster endpoint> \
  --bucket <bucket name> \
  --format <lines | list> \
  --username <username> \
  --password <password> \
  --output export.json \
  --include-key _id
```

Importe los datos a una colección de Amazon DocumentDB mediante mongoimport con la opción adecuada para importar las líneas o la lista:

líneas:

```
mongoimport \
  --db <database> \
  --collection <collection> \
  --uri "<Amazon DocumentDB cluster connection string>" \
  --file export.json
```

lista:

```
mongoimport \
  --db <database> \
  --collection <collection> \
  --uri "<Amazon DocumentDB cluster connection string>" \
  --jsonArray \
  --file export.json
```

De las colecciones de Couchbase a las colecciones de Amazon DocumentDB

Exporte los datos mediante cbexport json para crear un volcado de JSON de cada colección. Usa la `--include-data` opción para exportar cada colección. Para la `--format` opción, puede usar `lines` `olist`. Utilice las `--collection-field` opciones `--scope-field` y para almacenar el nombre del ámbito y la colección en los campos especificados de cada documento JSON.

```
cbexport json \
  --cluster <source cluster endpoint> \
  --bucket <bucket name> \
  --include-data <scope name>.<collection name> \
  --format <lines | list> \
  --username <username> \
  --password <password> \
  --output export.json \
  --include-key _id \
  --scope-field "_scope" \
  --collection-field "_collection"
```

Como cbexport agregó los `_collection` campos `_scope` y a todos los documentos exportados, puede eliminarlos de todos los documentos del archivo de exportación mediante la función de búsqueda y reemplazo`sed`, o mediante el método que prefiera.

Importe los datos de cada colección a una colección de Amazon DocumentDB mediante mongoimport con la opción adecuada para importar las líneas o la lista:

líneas:

```
mongoimport \
--db <database> \
--collection <collection> \
--uri "<Amazon DocumentDB cluster connection string>" \
--file export.json
```

lista:

```
mongoimport \
--db <database> \
--collection <collection> \
--uri "<Amazon DocumentDB cluster connection string>" \
--jsonArray \
```

```
--file export.json
```

Migración en línea

Considere la posibilidad de realizar una migración en línea cuando necesite minimizar el tiempo de inactividad y los cambios continuos deban replicarse en Amazon DocumentDB prácticamente en tiempo real.

Consulte Cómo realizar una migración en vivo de Couchbase a Amazon DocumentDB para obtener información sobre cómo realizar una migración en vivo a Amazon DocumentDB. La documentación explica cómo implementar la solución y realizar una migración en vivo de un bucket a un clúster de Amazon DocumentDB.

Temas

- Couchbase Server 6.x o anterior
- Couchbase Server 7.0 o posterior

Couchbase Server 6.x o anterior

De Couchbase a la colección Amazon DocumentDB

La utilidad de migración de Couchbase está preconfigurada para realizar una migración en línea de un bucket de Couchbase a una colección de Amazon DocumentDB. Si observamos la configuración del conector colector, el `document.id.strategy` parámetro está configurado para usar el valor de la clave del mensaje como valor de `_id` campo (consulte las propiedades de la estrategia del identificador del conector colector):

```
ConnectorConfiguration:
  document.id.strategy:
 'com.mongodb.kafka.connect.sink.processor.id.strategy.ProvidedInKeyStrategy'
```

Couchbase Server 7.0 o posterior

Depósito de Couchbase con alcance y colección predeterminados

La utilidad de migración de Couchbase está preconfigurada para realizar una migración en línea de un bucket de Couchbase a una colección de Amazon DocumentDB. Si observamos la configuración del conector colector, el `document.id.strategy` parámetro está configurado para usar el valor

de la clave del mensaje como valor de `_id` campo (consulte las propiedades de la estrategia del identificador del conector colector):

```
ConnectorConfiguration:
  document.id.strategy:
 'com.mongodb.kafka.connect.sink.processor.id.strategy.ProvidedInKeyStrategy'
```

De las colecciones de Couchbase a las colecciones de Amazon DocumentDB

Configure el conector de origen para transmitir cada colección de Couchbase de cada ámbito a un tema independiente (consulte las opciones de configuración de fuentes). Por ejemplo:

```
ConnectorConfiguration:
  # add couchbase.collections configuration
  couchbase.collections: '<scope 1>.<collection 1>, <scope 1>.<collection 2>, ...'
```

Configure el conector receptor para transmitir desde cada tema a una colección independiente de Amazon DocumentDB (consulte Propiedades de configuración del conector receptor). Por ejemplo:

```
ConnectorConfiguration:
  # remove collection configuration
  #collection: 'test'

  # modify topics configuration
  topics: '<bucket>.<scope 1>.<collection 1>, <bucket>.<scope 1>.<collection 2>, ...'

  # add topic.override.%s.%s configurations for each topic
  topic.override.<bucket>.<scope 1>.<collection 1>.collection: '<collection>'
  topic.override.<bucket>.<scope 1>.<collection 2>.collection: '<collection>'
```

Validación

En esta sección se proporciona un proceso de validación detallado para garantizar la coherencia e integridad de los datos tras la migración a Amazon DocumentDB. Los pasos de validación se aplican independientemente del método de migración.

Temas

- Compruebe que todas las colecciones existan en el destino
- Verifique el recuento de documentos entre los clústeres de origen y destino
- Compare documentos entre los clústeres de origen y destino

Compruebe que todas las colecciones existan en el destino

Fuente de Couchbase

opción 1: consulta el banco de trabajo

```
SELECT RAW `path`
  FROM system:keyspaces
  WHERE `bucket` = '<bucket>'
```

opción 2: herramienta cbq

```
cbq \
  -e <source cluster endpoint> \
  -u <username> \
  -p <password> \
  -q "SELECT RAW `path`
       FROM system:keyspaces
       WHERE `bucket` = '<bucket>'"
```

Amazon DocumentDB como destino

mongosh (consulte Conectarse a su clúster de Amazon DocumentDB):

```
db.getSiblingDB('<database>')
db.getCollectionNames()
```

Verifique el recuento de documentos entre los clústeres de origen y destino

Fuente de Couchbase

Couchbase Server 6.x o anterior

opción 1: consulta el banco de trabajo

```
SELECT COUNT(*)
FROM `<bucket>`
```

opción 2: cbq

```
cbq \
  -e <source cluster endpoint> \
  -u <username> \
  -p <password> \
  -q "SELECT COUNT(*)
       FROM `<bucket:>`"
```

Couchbase Server 7.0 o posterior

opción 1: consulta el banco de trabajo

```
SELECT COUNT(*)
FROM `<bucket>`.`<scope>`.`<collection>`
```

opción 2: cbq

```
cbq \
  -e <source cluster endpoint> \
  -u <username> \
  -p <password> \
  -q "SELECT COUNT(*)
       FROM `<bucket:>`.`<scope>`.`<collection>`"
```

Amazon DocumentDB como destino

mongosh (consulte Conectarse a su clúster de Amazon DocumentDB):

```
db = db.getSiblingDB('<database>')
db.getCollection('<collection>').countDocuments()
```

Compare documentos entre los clústeres de origen y destino

Fuente de Couchbase

Couchbase Server 6.x o anterior

opción 1: consulta el banco de trabajo

```
SELECT META().id as _id, *
FROM `<bucket>`
LIMIT 5
```

opción 2: cbq

```
cbq \
  -e <source cluster endpoint>
  -u <username> \
  -p <password> \
  -q "SELECT META().id as _id, *
       FROM `<bucket>` \
       LIMIT 5"
```

Couchbase Server 7.0 o posterior

opción 1: consulta el banco de trabajo

```
SELECT COUNT(*)
FROM `<bucket>`.`<scope>`.`<collection>`
```

opción 2: cbq

```
cbq \
  -e <source cluster endpoint> \
  -u <username> \
  -p <password> \
  -q "SELECT COUNT(*)
       FROM `<bucket:>`.`<scope>`.`<collection>`"
```

Amazon DocumentDB como destino

mongosh (consulte Conectarse a su clúster de Amazon DocumentDB):

```
db = db.getSiblingDB('<database>')
db.getCollection('<collection>').find({
  _id: {
    $in: [
      <_id 1>, <_id 2>, <_id 3>, <_id 4>, <_id 5>
    ]
  }
```

```
})
```

Actualización de Amazon DocumentDB

Inserte aquí su párrafo introductorio.

Temas

- Fechas de soporte de la versión del motor de Amazon DocumentDB
- Actualización local de la versión principal Amazon DocumentDB
- Actualización del clúster de Amazon DocumentDB mediante AWS Database Migration Service

Fechas de soporte de la versión del motor de Amazon DocumentDB

Amazon DocumentDB admite varias versiones de motores en el marco del soporte estándar. Puede seguir ejecutando una versión después de la fecha de finalización del soporte estándar con el pago de una tarifa por Soporte extendido. Para obtener más información, consulte Soporte extendido de Amazon DocumentDB y Precios de Amazon DocumentDB.

Puede utilizar las siguientes fechas para planificar sus ciclos de prueba y actualización.

Versión del motor	Fecha de lanzamiento de la nueva versión	Fecha de finalización del soporte estándar	Inicio del soporte extendido (precio del primer año)	Inicio del soporte extendido (precio del tercer año)	Fecha de finalización del soporte extendido
Versión 3.6	9 de enero de 2019	30 de marzo de 2026	31 de marzo de 2026	31 de marzo de 2028	30 de marzo de 2029
Versión 4.0	9 de noviembre de 2020	N/A	N/A	N/A	N/A
Versión 5.0	1 de marzo de 2023	N/A	N/A	N/A	N/A

Actualización local de la versión principal Amazon DocumentDB

Amazon DocumentDB hace que estén disponibles en las nuevas versiones del motor de base de datos solo después de realizar pruebas exhaustivas. Puede elegir cuándo y cómo actualizar sus clústeres de Amazon DocumentDB a la nueva versión.

Actualmente, Amazon DocumentDB admite cuatro versiones principales: Amazon DocumentDB 3.6, 4.0, 5.0 y 8.0. Puede realizar una actualización inmediata de la versión principal (MVU) de la base de datos y, al mismo tiempo, conservar los mismos puntos de conexión, almacenamiento y etiquetas de los clústeres, y seguir utilizando las aplicaciones sin necesidad de realizar modificaciones. Esta característica está disponible de forma gratuita en todas las regiones en las que Amazon DocumentDB 5.0 está disponible. Nota: Actualmente, MVU no es compatible con Amazon DocumentDB 8.0.

> **Important**
>
> Los clústeres de Amazon DocumentDB no estarán disponibles durante la actualización de la versión principal y los clústeres se reiniciarán varias veces. Absténgase de conectarse al clúster o leer y escribir en el clúster después de iniciar la actualización. El tiempo de inactividad de la actualización puede variar de un clúster a otro en función del número de colecciones, índices, bases de datos e instancias. Recomendamos realizar la actualización durante el período de mantenimiento o durante las horas de baja utilización. Una vez actualizado el clúster, no puede cambiarlo a una versión anterior, pero puede optar por restaurar la instantánea previa a la actualización en un clúster nuevo.

Temas

- Requisitos previos y limitaciones de la MVU
- Prácticas recomendadas para actualizaciones de la versión principal locales
- Actualización local de la versión principal
- Diferencias entre los clústeres actualizados de Amazon DocumentDB 3.6 o 4.0 a 5.0 y los nuevos clústeres de Amazon DocumentDB 5.0
- Solución de problemas de una actualización local de la versión principal

Requisitos previos y limitaciones de la MVU

A continuación se indican los requisitos previos y las limitaciones de la actualización de la versión principal que tal vez deba comprender y cumplir antes de realizar la actualización: (Nota: actualmente, MVU no es compatible con Amazon DocumentDB 8.0).

- Tipo de instancia: Amazon DocumentDB 4.0/5.0 no admite instancias r4.*. Para continuar con la actualización inmediata de la versión principal, cambie las instancias r4.* por las instancias r5.*. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon DocumentDB. Consulte las Clases de instancias admitidas por región instancias compatibles basadas en la versión del motor Amazon DocumentDB.
- Parches del sistema operativo de la instancia: una actualización de una versión principal implementada necesita el último parche del sistema operativo (SO) para continuar. Aplique todas las acciones pendientes de mantenimiento del sistema operativo a las instancias antes de continuar con la actualización local. Para obtener más información, consulte Actualizaciones del sistema operativo de Amazon DocumentDB.

  > **Note**
  >
  > En algunas situaciones, si tiene parches de motor pendientes a nivel de clúster, los parches del sistema operativo de la instancia no están visibles. Quizá tenga que aplicar los parches del motor a nivel de clúster antes de proceder a aplicar los parches del sistema operativo de la instancia y, posteriormente, realizar la actualización de la versión principal ya implementada. Consulte Actualización de un parche a la versión del motor de un clúster.

- La actualización local de la versión principal está disponible en todas las regiones en las que Amazon DocumentDB 5.0 está disponible.
- La actualización local de la versión principal no es compatible con Amazon DocumentDB 4.0 como versión de destino.
- A partir de Amazon DocumentDB 4.0, no se admite “.” en los nombres de usuario. Si se está actualizando de Amazon DocumentDB 3.6 a 5.0 y tiene un nombre de usuario que contiene “.”, vuelva a crear su nombre de usuario sin “.” antes de continuar con la MVU local.
- La actualización local de la versión principal no se admite actualmente en los clústeres globales y elásticos de Amazon DocumentDB.

> **Note**
>
> Para actualizar los clústeres globales, elimine los clústeres secundarios del clúster global, convierta el clúster principal en un clúster regional, actualice la versión principal local del clúster regional (principal) y, a continuación, vuelva a crear el clúster global añadiendo clústeres secundarios con el mismo nombre para conservar los mismos puntos de conexión que antes. Tenga en cuenta que incurrirá en gastos de IO mientras el clúster principal actualizado replique los datos en los clústeres secundarios recién agregados. Para ver los pasos detallados sobre cómo eliminar los clústeres secundarios del clúster global antes de eliminarlos, consulte Eliminación de un clúster global de Amazon DocumentDB.

- Si tiene una gran cantidad de índices (más de 3000) y opera en una instancia de rendimiento ampliable (por ejemplo, t3.medium o t4g.medium), debe escalar verticalmente la instancia principal a una instancia más grande (por ejemplo, al menos r5.xlarge) para llevar a cabo la actualización local de la versión principal. Puede optar por reducir verticalmente el tamaño de la instancia una vez que se haya completado la actualización local de la versión principal. Consulte la siguiente tabla para ver el número máximo de índices admitidos en los tipos de instancias db.t3 y db.t4g para una actualización local de la versión principal:

Instancia	Índices máximos admitidos para la MVU local
db.t4g.medium	3,000
db.t3.medium	10,000

Prácticas recomendadas para actualizaciones de la versión principal locales

Temas

- Prueba de las actualizaciones locales de la versión principal mediante clústeres clonados
- Antes de una actualización local de la versión principal
- Durante una actualización local de la versión principal
- Después de una actualización local de la versión principal

Prueba de las actualizaciones locales de la versión principal mediante clústeres clonados

1. Para probar las actualizaciones de las versiones principales locales, le recomendamos que utilice la característica de clonación rápida para crear un clon del clúster de destino. No incurrirá en ningún costo de almacenamiento por probar la actualización local de la versión principal en un volumen clonado, a menos que modifique los datos del clúster. Para obtener más información acerca de la clonación, consulte Clonación de un volumen de clúster de base de datos de Amazon DocumentDB.
2. Para obtener una estimación más realista del tiempo necesario para completar la actualización local de la versión principal, haga coincidir el número de instancias del clúster clonado con el clúster de destino.
3. Recomendamos probar completamente el clúster Amazon DocumentDB 5.0 recién actualizado para detectar cualquier diferencia funcional a fin de garantizar que todo funcione según lo esperado.

Antes de una actualización local de la versión principal

1. Tenga preparado un grupo de parámetros de clúster compatible con la versión.

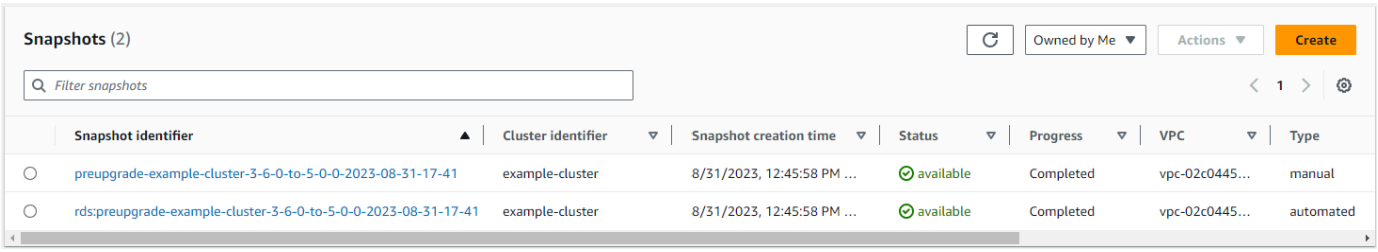
   Utilice el grupo de parámetros de clúster predeterminado de Amazon DocumentDB para la nueva versión del motor o cree su propio grupo de parámetros de clúster personalizado para la nueva versión del motor.

   Si asocia un grupo de parámetros de clúster de Amazon DocumentDB como parte de la solicitud de actualización, la actualización local de la versión principal Amazon DocumentDB como parte de la solicitud de actualización, la actualización local de la versión principal Amazon DocumentDB para aplicar el nuevo grupo de parámetros.
2. Asegúrese de cumplir los requisitos previos para una actualización local de la versión principal, tal como se menciona en la sección Requisitos previos y limitaciones.
3. Para crear una instantánea manual.

   El proceso de actualización crea una instantánea del clúster de base de datos durante la actualización. Se recomienda encarecidamente crear su propia instantánea manual antes del proceso de actualización. Consulte Creación de una instantánea manual del clúster.

> **Note**
>
> La instantánea automática creada por el proceso de actualización no se eliminará automáticamente una vez que se haya completado la actualización local de la versión principal. Esta instantánea no incurrirá en ningún cargo mientras se encuentre dentro del período de retención. Puede optar por eliminar esta instantánea una vez que haya comprobado que la actualización del clúster se ha realizado correctamente.

La instantánea se denomina `preupgrade-<name>-<version>-<timestamp>`.



4. Compruebe si ya ha programado una actualización local de la versión principal de su clúster.

   Si ha modificado el clúster y ha seleccionado aplicarlo en la siguiente ventana de mantenimiento, el programa de actualización de la versión principal vigente no estará visible en la consola, pero podrá verlo en la CLI. Puede ejecutar el comando `describe-db-clusters` para comprobar si ya hay una actualización local de la versión principal programada:

   ```
   aws docdb describe-db-cluster \
     --region us-east-1 \
     --db-cluster-identifier mydocdbcluster
   ```

   En el ejemplo anterior, sustituya cada uno por la información de su *`user input placeholder`* clúster.

   El comando devuelve el siguiente resultado:

   ```
   "PendingModifiedValues": {
       "EngineVersion": "5.0.0"
   },
   ```

5. Realice varias ejecuciones en seco utilizando un clon de volumen en entornos más bajos para probar el clúster tras la actualización local de la versión principal en función de cualquier plan de

ejecución y diferencias funcionales. Recomendamos clonar con el mismo número y tamaño de instancias para obtener una mejor estimación del tiempo de ejecución de la actualización local de la versión principal. Para obtener más información, consulte Clonación de un volumen de clúster de base de datos de Amazon DocumentDB.

6. Si el paso anterior se realiza correctamente, continúe con la actualización local de la versión principal en el clúster de producción.

Durante una actualización local de la versión principal

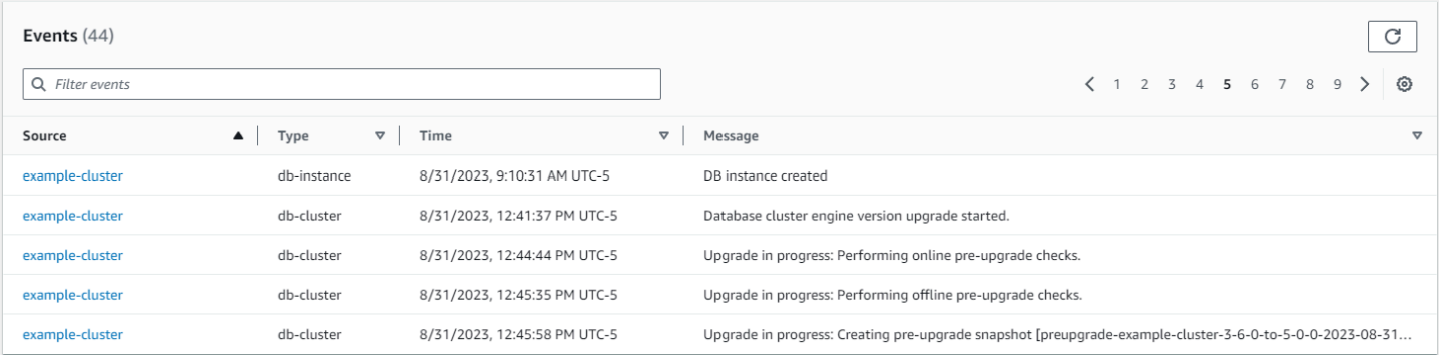
Puede supervisar el progreso de la actualización local de la versión principal suscribiéndose a los eventos de mantenimiento del clúster. Cuando se complete la actualización, recibirá el evento “Se ha actualizado la versión principal del clúster de bases de datos”. Este y otros eventos que se producen durante la actualización aparecen en la sección “Eventos y etiquetas” de la página de detalles del clúster en la consola de Amazon DocumentDB. A continuación, el estado del clúster cambia de “actualizado” a “disponible”.

Desde la CLI, puede ejecutar `aws docdb create-event-subscription` para crear eventos y `aws docdb describe-events` para monitorear el progreso. También puede configurar las notificaciones de eventos para los eventos anteriores a Amazon SNS como destino para recibir las notificaciones por correo electrónico, mensajes push y otros métodos. Para obtener más información, consulte Suscripción a eventos de Amazon DocumentDB.

La actualización local de la versión principal genera los siguientes eventos durante la actualización:

- Actualización en curso: creación de una instantánea previa a la actualización [preupgrade-<cluster-name>-<timestamp>]
- Actualización en curso: volumen de clonación.
- Actualización en curso: actualización del escritor.
- Actualización en curso: actualización de los lectores.
- Se ha actualizado la versión principal del motor de clústeres de bases de datos.

Los eventos también están visibles en la consola, en la página Eventos:



En el AWS CLI, puedes ejecutar el `describe-events`comando para hacer un seguimiento del progreso:

```
aws docdb describe-events
  --source-identifier mydocdbcluster
  --source-type db-cluster
```

En el ejemplo anterior, sustituya cada uno *`user input placeholder`* por la información de su clúster.

El comando devuelve el siguiente resultado:

```
{
    "Events": [
        {
            "SourceIdentifier": "mydocdbcluster",
            "SourceType": "db-cluster",
            "Message": "Database cluster engine version upgrade started.",
            "EventCategories": [
                "maintenance"
            ],
            "Date": "2023-07-11T23:20:32.444000+00:00",
            "SourceArn": "arn:aws:rds:us-east-1:xxxx:cluster:mycluster"
        }
    ]
}
```

Después de una actualización local de la versión principal

Para Amazon DocumentDB 3.6, añada una etiqueta al clúster para diferenciar que el clúster se actualizó a Amazon DocumentDB 5.0 desde Amazon DocumentDB 3.6 y no a un clúster de Amazon

DocumentDB 5.0 recién creado. Consulte la sección sobre las diferencias entre un clúster de Amazon DocumentDB 5.0 actualizado y un clúster de Amazon DocumentDB 5.0 nuevo.

Realice una instantánea manual cuando finalice la MVU en caso de que necesite restaurarla al estado posterior a la actualización. El proceso de creación automática de instantáneas se reanudará en cuanto se complete la actualización local de la versión principal. La instantánea manual no incurrirá en ningún cargo mientras se encuentre dentro del período de retención.

Para utilizar las nuevas funciones asociadas a Amazon DocumentDB 5.0, por ejemplo, el cifrado a nivel de campo del lado del cliente, le recomendamos que actualice la versión del controlador a la versión de la API de MongoDB 5.0. Para obtener más información, consulte Novedades de Amazon DocumentDB 5.0 para ver una la lista de características de Amazon DocumentDB 5.0.

Important

Inmediatamente después de hacer la actualización local de la versión principal (MVU), el clúster de Amazon DocumentDB 5.0 rellenará los metadatos del índice, en función de los cuales el motor de base de datos optimiza los planes de ejecución de las consultas. El rendimiento esperado de las consultas en el clúster de Amazon DocumentDB se reanudará una vez finalizado el proceso de recálculo de los metadatos del índice. Por lo general, este proceso se completa en unos minutos, pero puede durar hasta dos horas, según la cantidad de índices del clúster. Un reinicio inmediato, una conmutación por error o una escala up/down de la instancia de grabación tras instalar la MVU podría interrumpir el proceso de cálculo de los metadatos del índice en el clúster. Una vez finalizada la MVU local, le recomendamos que haga dichos cambios una vez que observe el rendimiento esperado de las consultas en el clúster de Amazon DocumentDB 5.0.
Puede realizar un seguimiento del inicio y el final de este proceso de recálculo mediante los siguientes eventos del clúster:

- Estado del clúster posterior a la actualización: se inició el proceso de actualización de los metadatos del índice
- Estado del clúster posterior a la actualización: el proceso de actualización de los metadatos del índice se completó en X segundos

Póngase en contacto con el servicio de AWS asistencia si el proceso de actualización de los metadatos del índice no se ha completado en tres horas o si sigue teniendo problemas de rendimiento una vez finalizado el proceso.

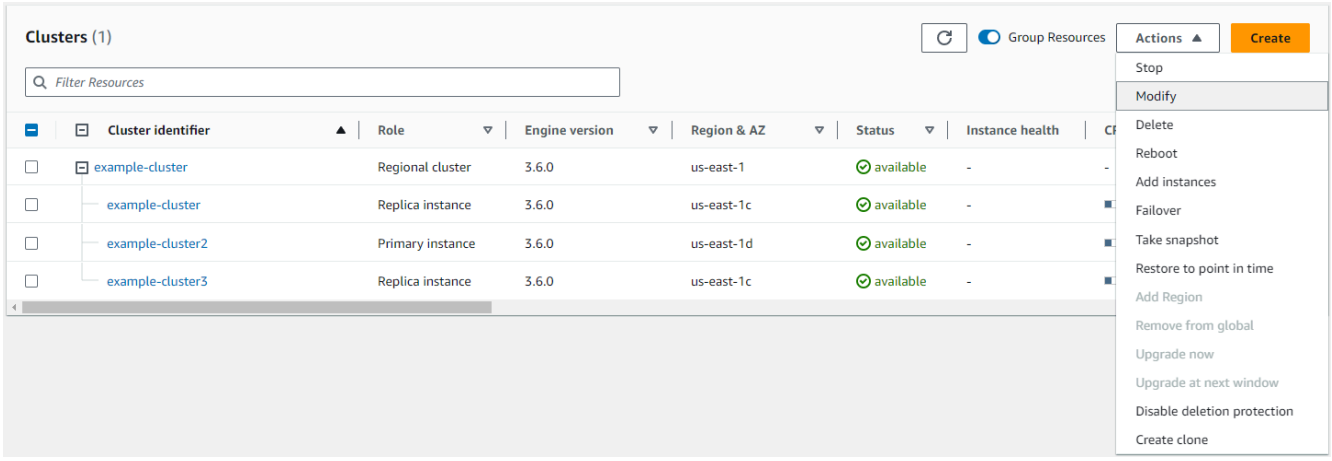
Pruebe completamente el clúster actualizado de Amazon DocumentDB 5.0 para asegurarse de que todo funciona según lo esperado.

Actualización local de la versión principal

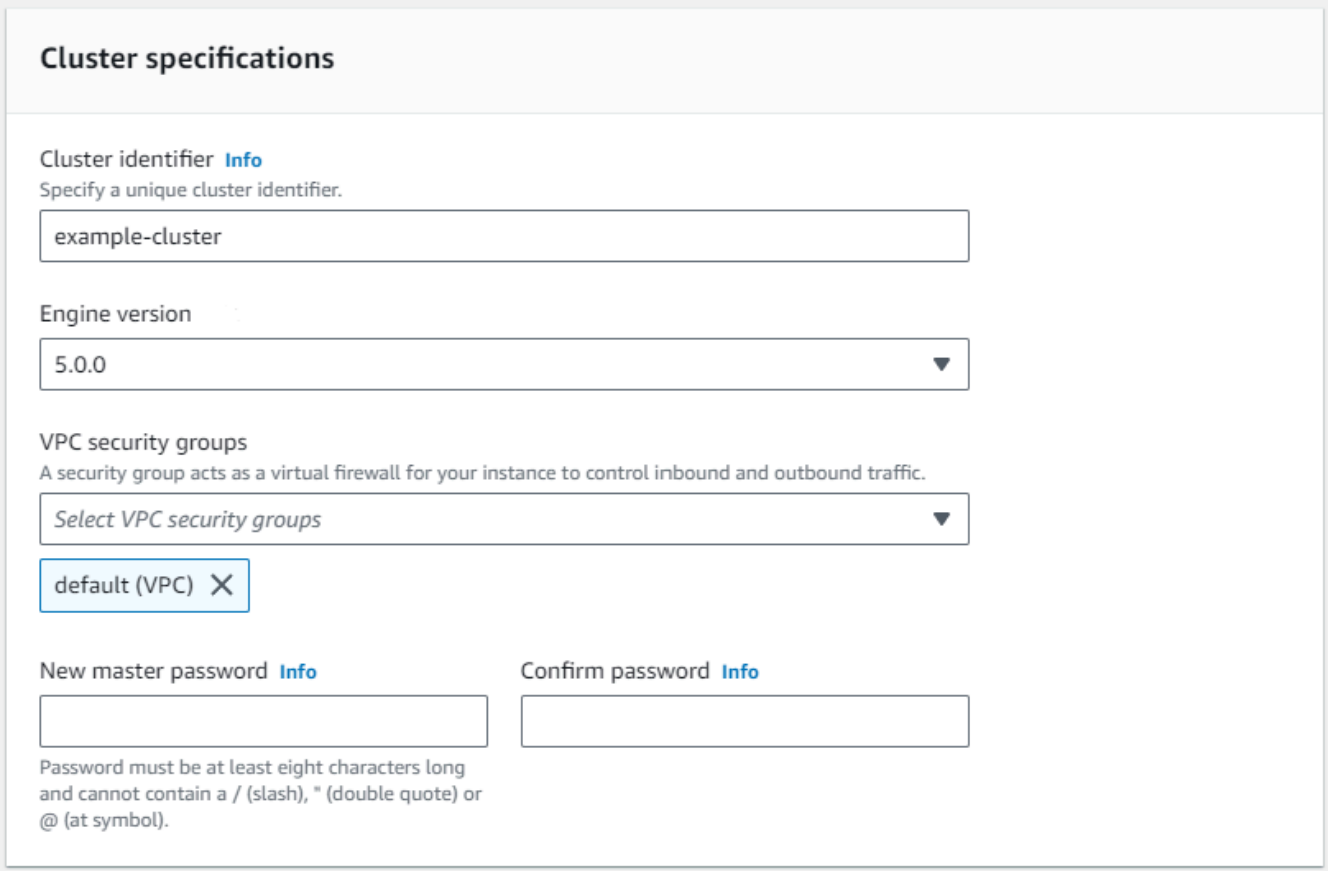
Using the Consola de administración de AWS

Para realizar una actualización local de la versión principal usando la Consola de administración de AWS:

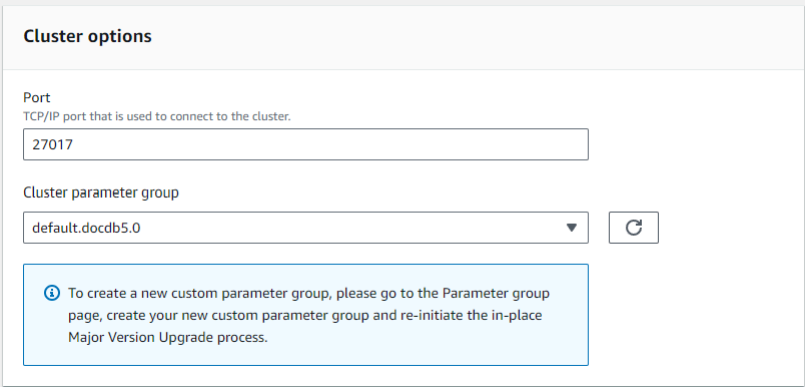
1. Inicie sesión en la Consola de administración de AWS de Amazon DocumentDB y ábrala.
2. En la tabla Clústeres, seleccione el clúster de origen, haga clic en Acciones y, a continuación, en Modificar.



3. En el cuadro de diálogo Modificar clúster, en la sección Especificaciones del clúster, elija la versión de la base de datos de destino (5.0.0) en el menú desplegable Versión del motor.

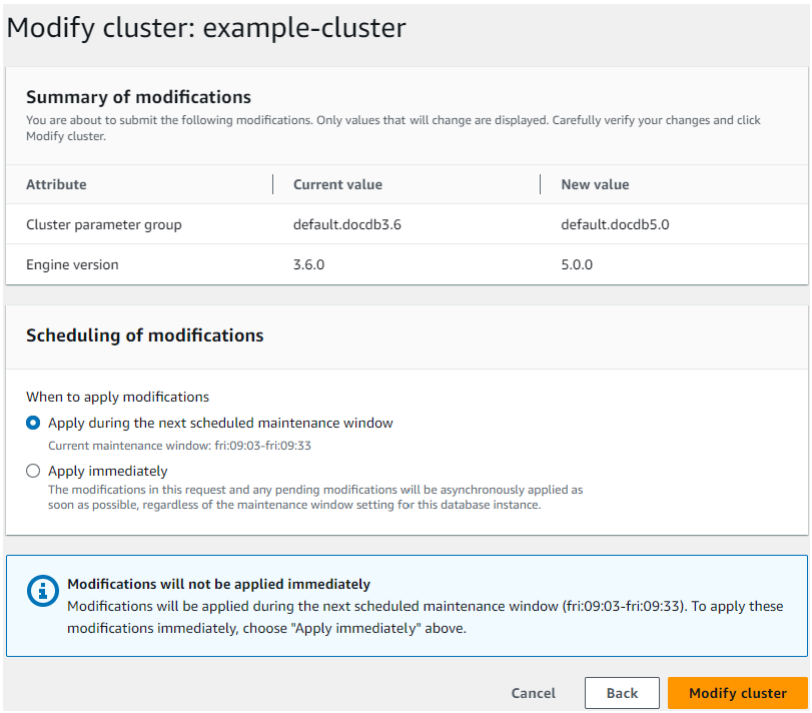


4. En la sección Opciones de clúster, elija el grupo de parámetros de clúster adecuado (default.docdb5.0) o un grupo de parámetros creado de forma personalizada.

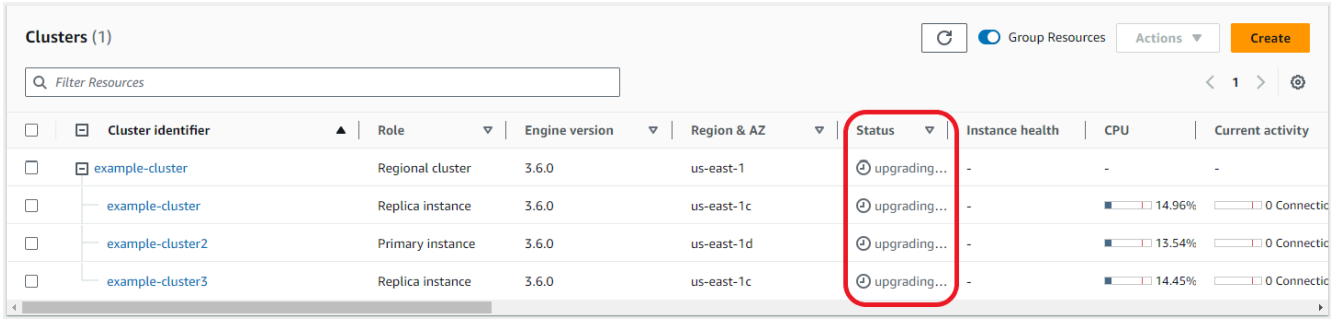


5. Cuando haya terminado, desplácese hacia abajo y elija Continuar.
6. En la sección Programación de modificaciones, elija el plan de programación que prefiera: solicítelo inmediatamente o solicítelo en el siguiente período de mantenimiento.

   A continuación, seleccione Modify cluster (Modificar clúster).



7. En la tabla Clústeres, anote el estado del clúster a medida que se actualiza:



Using the AWS CLI

Use el comando [modify-db-cluster](#) con la versión de motor deseada y el conjunto de indicadores `allow-major-version-upgrade`:

```
aws docdb modify-db-cluster \
  --db-cluster-identifier mydocdbcluster \
  --allow-major-version-upgrade \
  --engine-version 5.0.0 \
  --apply-immediately \
  --cluster-parameter-group mydocdbparametergroup \
  --region us-east-1
```

En el ejemplo anterior, sustituye cada uno *`user input placeholder`* por la información de tu clúster.

Diferencias entre los clústeres actualizados de Amazon DocumentDB 3.6 o 4.0 a 5.0 y los nuevos clústeres de Amazon DocumentDB 5.0

- Una actualización local de la versión principal conserva los índices originales del clúster actualizado. Con Amazon DocumentDB 5.0, hemos mejorado la eficiencia general del mantenimiento del índice y del proceso de recopilación de elementos no utilizados, especialmente para los índices de cardinalidad bajos. Como práctica recomendada general, recomendamos recrear los índices con el comando reindexar una vez que la MVU se haya completado correctamente. La recreación de los índices no es obligatoria e implicará E/S adicionales. Para obtener más información, consulte Mantenimiento de índices mediante `reIndex`.
- Comparaciones de subdocumentos para varios tipos de datos numéricos:
  - Si el clúster se migra desde Amazon DocumentDB 3.6, heredará el comportamiento de comparación de subdocumentos de Amazon DocumentDB 3.6. La diferencia funcional se limita a los tipos numéricos (como Long, Double o Decimal128) en un subdocumento. Por ejemplo, `{a: {b: {NumberLong(1)}}` no es igual que `{a: {b: 1}}` en Amazon DocumentDB 3.6, mientras que se comparan como iguales en Amazon DocumentDB 4.0 y versiones posteriores.
  - Este comportamiento de comparación de subdocumentos solo existe en los clústeres de Amazon DocumentDB 3.6 y Amazon DocumentDB 5.0 que se actualizaron desde la versión 3.6 mediante una actualización local de la versión principal. Esto no se aplica a los clústeres de Amazon DocumentDB 5.0 recién creados.

> **Note**
>
> Para obtener una lista de las diferencias funcionales entre Amazon DocumentDB 3.6/4.0 y Amazon DocumentDB 5.0, consulte Compatibilidad de Amazon DocumentDB con MongoDB.

Solución de problemas de una actualización local de la versión principal

- En caso de que se produzca un error, la actualización local de la versión principal intentará anular la actualización para adoptar el último estado operativo del clúster antes de que se iniciara la actualización. Una reversión correcta generará un evento: “El clúster de base de datos está en un

estado que no se puede actualizar: el clúster de DocumentDB se encuentra en un estado en el que la actualización de la versión principal no se puede completar correctamente". En este punto, debes ponerte en contacto con el equipo de AWS soporte para solucionar el problema y volver a intentar la actualización de la versión. Puede seguir utilizando su carga de trabajo como antes. En cualquier otro caso poco frecuente en el que la actualización tarde más de lo esperado, ponte en contacto con el equipo de AWS soporte para obtener ayuda.

- Una vez que la MVU local se complete correctamente, es posible que el clúster actualizado experimente una degradación temporal del rendimiento y un alto uso de la CPU durante un breve periodo de tiempo mientras se ejecuta el proceso de actualización de los metadatos del índice. Si sigues experimentando una degradación del rendimiento durante más de 2 horas, ponte en contacto con el servicio de AWS asistencia.

Actualización del clúster de Amazon DocumentDB mediante AWS Database Migration Service

> **Important**
>
> Amazon DocumentDB no sigue los mismos ciclos de vida de soporte que MongoDB y el cronograma de MongoDB no se aplica a Amazon DocumentDB end-of-life.

Puede actualizar su clúster de Amazon DocumentDB a una versión superior con un tiempo de inactividad mínimo utilizando. AWS DMS AWS DMS es un servicio totalmente gestionado que facilita la migración desde versiones anteriores de Amazon DocumentDB, bases de datos relacionales y bases de datos no relacionales al clúster de Amazon DocumentDB de destino.

Temas

- Paso 1: habilitación de los flujos de cambios
- Paso 2: modificación de la duración de la retención de los flujos de cambios
- Paso 3: migración de los índices
- Paso 4: Crear una AWS DMS instancia de replicación
- Paso 5: Crear un punto final AWS DMS de origen
- Paso 6: Crear un punto final AWS DMS de destino
- Paso 7: crear y ejecutar una tarea de migración

- Paso 8: cambiar el punto de conexión de origen de la aplicación al clúster de Amazon DocumentDB de destino

Paso 1: habilitación de los flujos de cambios

Para realizar una migración con un tiempo de inactividad mínimo, AWS DMS requiere acceso a los flujos de cambios del clúster. La secuencia de cambios de Amazon DocumentDB brinda una secuencia en orden cronológico de los eventos de actualización que se producen dentro de las colecciones y bases de datos de su clúster. La lectura del flujo de cambios permite AWS DMS realizar una captura de datos de cambios (CDC) y aplicar actualizaciones incrementales al clúster de Amazon DocumentDB de destino.

Para habilitar las secuencias de cambios para todas las colecciones de una base de datos específica, autentíquese en su clúster de Amazon DocumentDB mediante el shell de mongo y ejecute los siguientes comandos:

```
db.adminCommand({modifyChangeStreams: 1,
    database: "db_name",
    collection: "",
    enable: true});
```

Paso 2: modificación de la duración de la retención de los flujos de cambios

A continuación, modifique el período de retención de la secuencia de cambios en función del tiempo que desee conservar los eventos de cambio en la secuencia de cambios. Por ejemplo, si espera que la migración del clúster de Amazon DocumentDB AWS DMS tarde 12 horas, debe establecer la retención del flujo de cambios en un valor superior a 12 horas. El periodo de retención predeterminado para el clúster de Amazon DocumentDB es de tres horas. Puede modificar la duración de retención del registro de flujos de cambios de su clúster de Amazon DocumentDB para que oscile entre una hora y siete días utilizando el Consola de administración de AWS o el. AWS CLI Para obtener más información, consulte Modificación de la duración de retención del registro de la secuencia de cambios.

Paso 3: migración de los índices

Cree los mismos índices en el clúster de Amazon DocumentDB de destino que en el clúster de Amazon DocumentDB de origen. Si bien AWS DMS gestiona la migración de datos, no migra los índices. Para migrar los índices, utilice la herramienta de índices de Amazon DocumentDB para

exportar los índices del clúster de Amazon DocumentDB de origen. Para obtener la herramienta, cree un clon del GitHub repositorio de herramientas de Amazon DocumentDB y siga las instrucciones que se indican en. `README.md` Puede ejecutar la herramienta desde una EC2 instancia de Amazon o desde un AWS Cloud9 entorno que se ejecute en la misma Amazon VPC que su clúster de Amazon DocumentDB.

Para utilizar el ejemplo siguiente, sustituya *`user input placeholder`* con su propia información.

El siguiente código descarga los índices del clúster de Amazon DocumentDB de origen:

```
python migrationtools/documentdb_index_tool.py --dump-indexes
--uri mongodb://sample-user:user-password@sample-source-cluster.node.us-
east 1.docdb.amazonaws.com:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false'
--dir ~/index.js/

2020-02-11 21:51:23,245: Successfully authenticated to database: admin2020-02-11
 21:46:50,432: Successfully connected to instance docdb-40-xx.cluster-xxxxxxxx.us-
east-1.docdb.amazonaws.com:27017
2020-02-11 21:46:50,432: Retrieving indexes from server...2020-02-11 21:46:50,440:
 Completed writing index metadata to local folder: /home/ec2-user/index.js/
```

Una vez que los índices se hayan exportado correctamente, restaure esos índices en el clúster de Amazon DocumentDB de destino. Para restaurar los índices que exportó en el paso anterior, utilice la herramienta de índices de Amazon DocumentDB. El siguiente comando restaura los índices del clúster de Amazon DocumentDB de destino desde el directorio especificado.

```
python migrationtools/documentdb_index_tool.py --restore-indexes
--uri mongodb://sample-user:user-password@sample-destination-
cluster.node.us-east 1.docdb.amazonaws.com:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false'
--dir ~/index.js/

2020-02-11 21:51:23,245: Successfully authenticated to database: admin2020-02-11
 21:51:23,245: Successfully connected to instance docdb-50-xx.cluster-xxxxxxxx.us-
east-1.docdb.amazonaws.com:27017
2020-02-11 21:51:23,264: testdb.coll: added index: _id
```

Para confirmar que restauró los índices correctamente, conéctese al clúster de Amazon DocumentDB de destino con el shell de mongo y enumere los índices de una colección determinada. Consulte el siguiente código:

```
mongo --ssl
--host docdb-xx-xx.cluster-xxxxxxxx.us-east-1.docdb.amazonaws.com:27017
--sslCAFile rds-ca-2019-root.pem --username documentdb --password documentdb

db.coll.getIndexes()
```

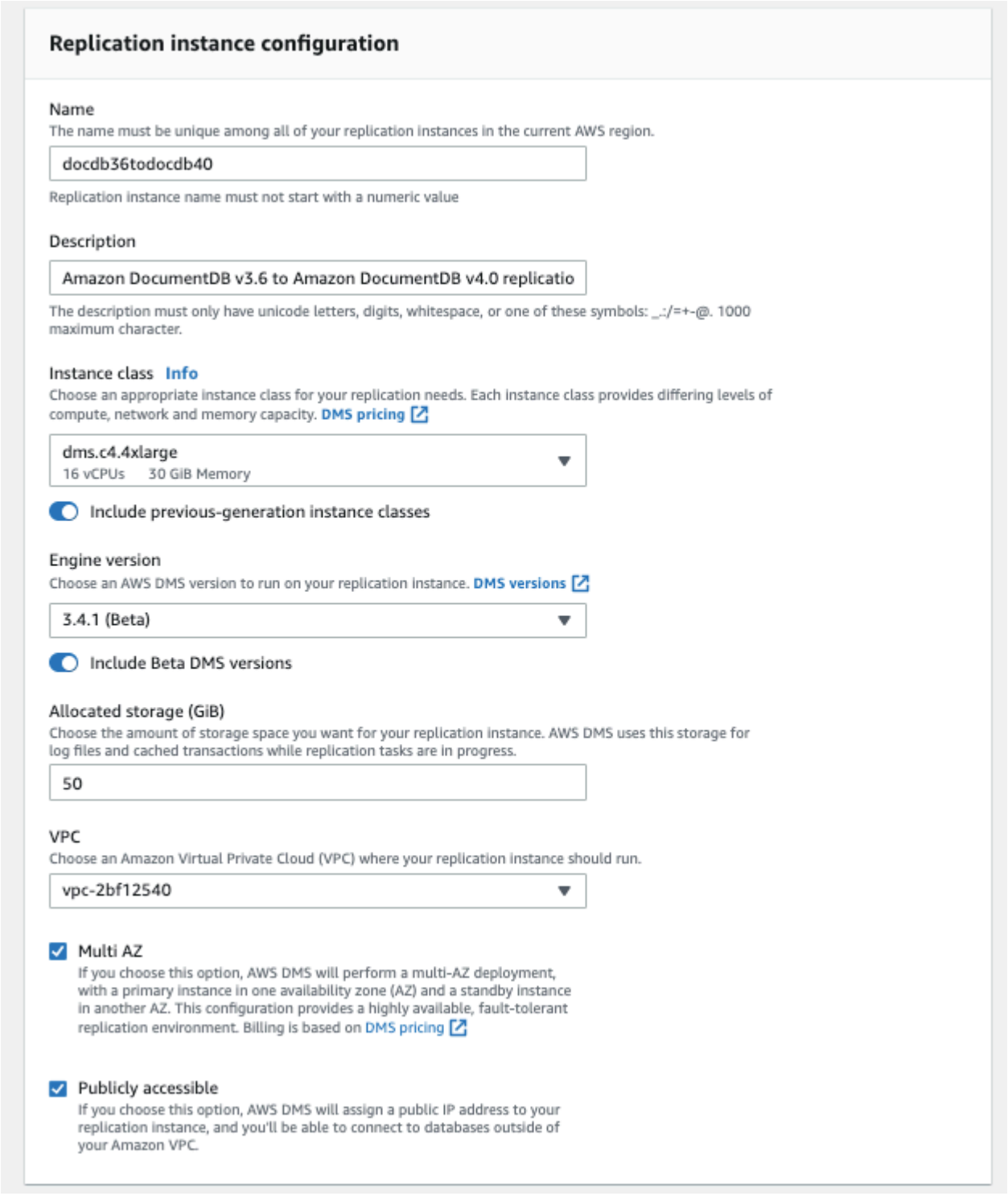
Paso 4: Crear una AWS DMS instancia de replicación

Una instancia de AWS DMS replicación conecta y lee los datos del clúster de Amazon DocumentDB de origen y los escribe en el clúster de Amazon DocumentDB de destino. La instancia de AWS DMS replicación puede realizar tanto operaciones de carga masiva como de CDC. La mayor parte de este procesamiento ocurre en la memoria. No obstante, es posible que en las operaciones de mayor volumen se precise almacenar en la memoria búfer del disco. Las transacciones almacenadas en caché y los archivos de registro también se escriben en el disco. Una vez que se migran los datos, la instancia de replicación también transmite cualquier evento de cambio para asegurarse de que el origen y el destino estén sincronizados.

Para crear una instancia AWS DMS de replicación:

1. Abra la AWS DMS consola.
2. En el panel de navegación, elija Instancias de replicación.
3. Elija Create replication instance (Crear instancia de replicación) y escriba la siguiente información:

   - En Nombre, escriba un nombre de su elección. Por ejemplo, `docdb36todocdb40`.
   - En Descripción, introduzca una descripción de su preferencia. En listitem, instancia de replicación de Amazon DocumentDB 3.6 a Amazon DocumentDB 4.0.
   - En la clase de instancia, elija el tamaño según sus necesidades.
   - En la versión Engine, elija `3.4.1.`
   - En el caso de Amazon VPC, elija la Amazon VPC que aloja los clústeres de Amazon DocumentDB de origen y destino.
   - Para el Almacenamiento asignado (GiB), utilice el valor predeterminado de 50 GiB. Si tiene una carga de trabajo de alto rendimiento de escritura, aumente este valor para que se adapte a su carga de trabajo.
   - Para Multi-AZ, elija Sí si necesita alta disponibilidad y soporte de conmutación por error.
   - En Publicly accessible (Accesible públicamente), habilite esta opción.



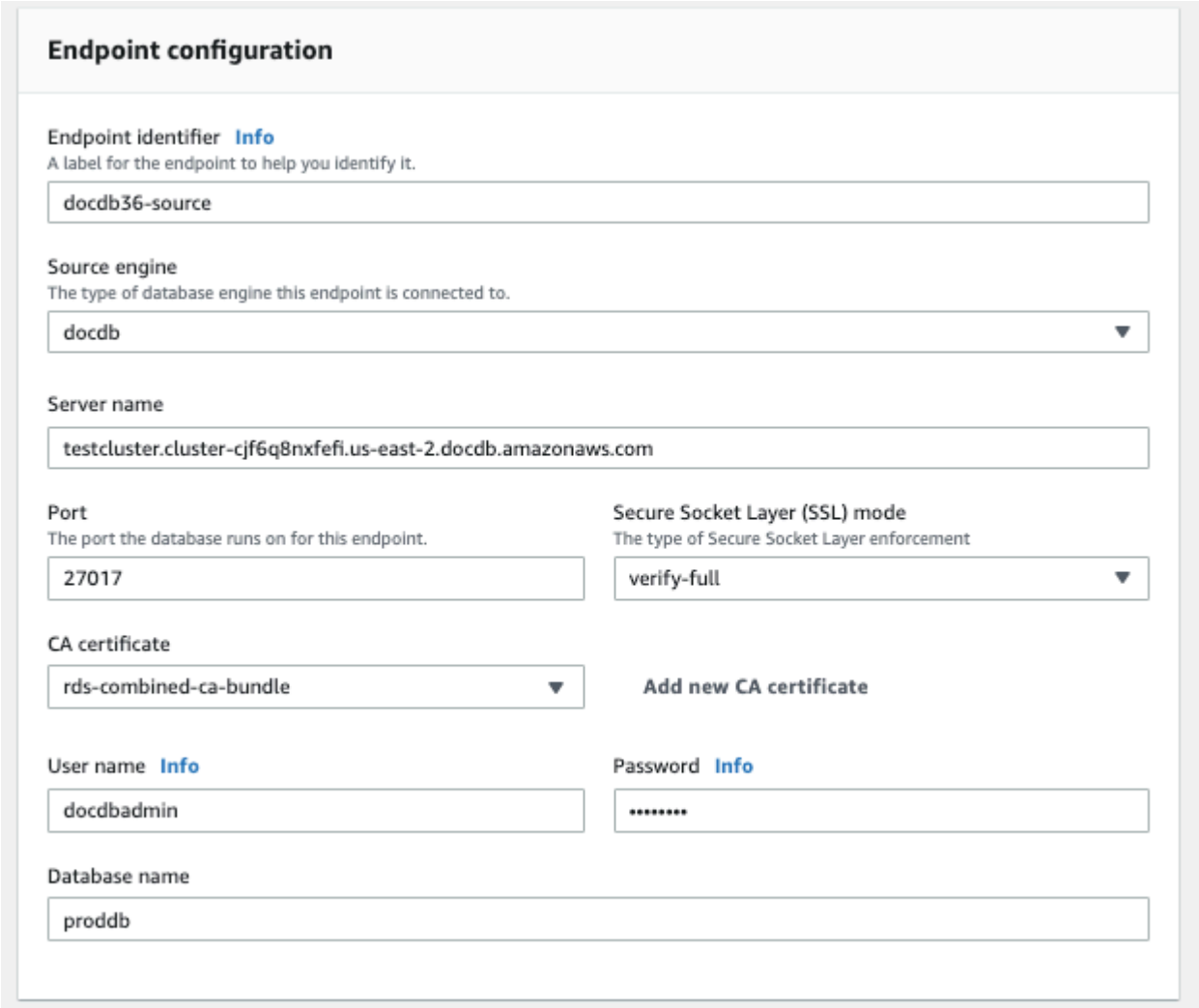
4. Elija Create replication instance.

Paso 5: Crear un punto final AWS DMS de origen

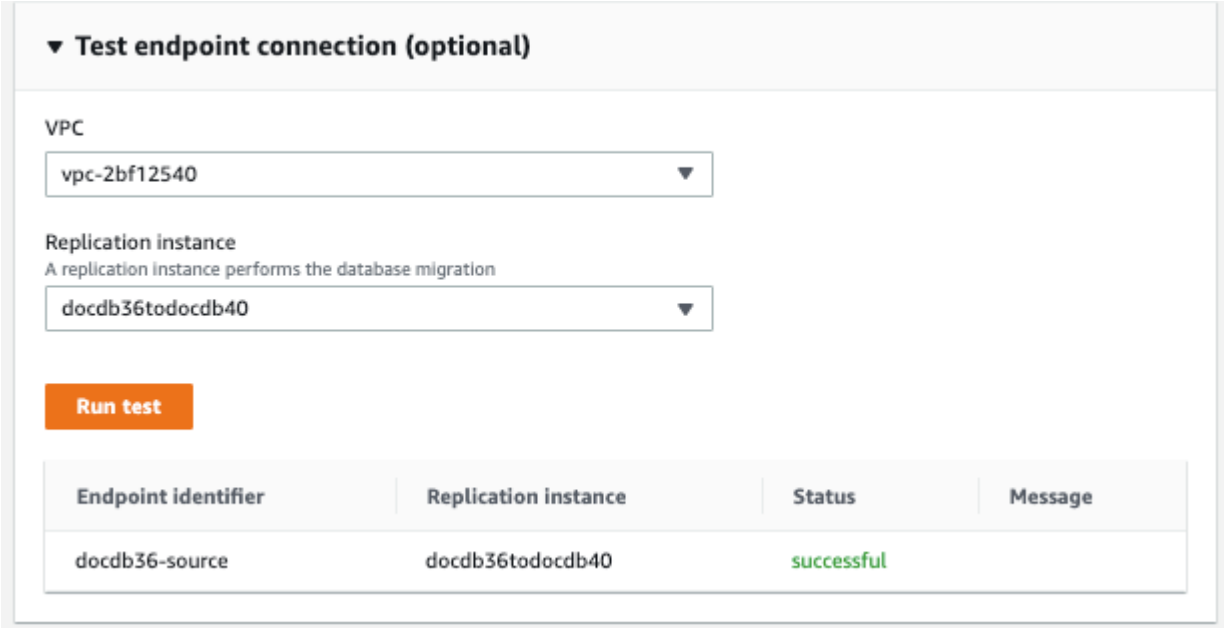
El punto de conexión de origen se utiliza para el clúster Amazon DocumentDB de origen.

Creación de un punto de conexión de origen

1. Abre la AWS DMS consola.
2. En el panel de navegación, elija Puntos de conexión.
3. Elija `Create endpoint` y especifique la siguiente información:
   - En Tipo de punto de conexión, elija Source (Origen).
   - >En Identificador de punto de conexión, escriba un nombre que sea fácil de recordar, como `docdb-source`.
   - En Motor de origen, seleccione `docdb`.
   - En Nombre de servidor, escriba el nombre DNS de su clúster de Amazon DocumentDB de origen.
   - En Puerto, escriba el número de puerto de su clúster de Amazon DocumentDB.
   - En Modo de SSL, elija `verify-full`.
   - En Certificado de CA, seleccione Añadir un nuevo certificado de CA. Descargue el nuevo certificado de CA, el nuevo certificado para crear el paquete de conexiones TLS. En Identificador del certificado, escriba `rds-combined-ca-bundle` . En Importar archivo de certificado, elija Seleccionar archivo y acceda al archivo `.pem` que descargó anteriormente. Seleccione el archivo y ábralo. Elija Importar certificado y luego elija `rds-combined-ca-bundle` de Elija un certificado.
   - En Nombre de usuario, escriba el nombre de usuario principal del clúster de Amazon DocumentDB de origen.
   - En Contraseña, escriba la contraseña principal del clúster de Amazon DocumentDB de origen.
   - En Nombre de la base de datos, introduzca el nombre de la base de datos que desee actualizar.



4. Pruebe su conexión para comprobar que se configuró correctamente.



5. Seleccione Crear punto de conexión.

> **Note**
>
> AWS DMS solo puede migrar una base de datos a la vez.

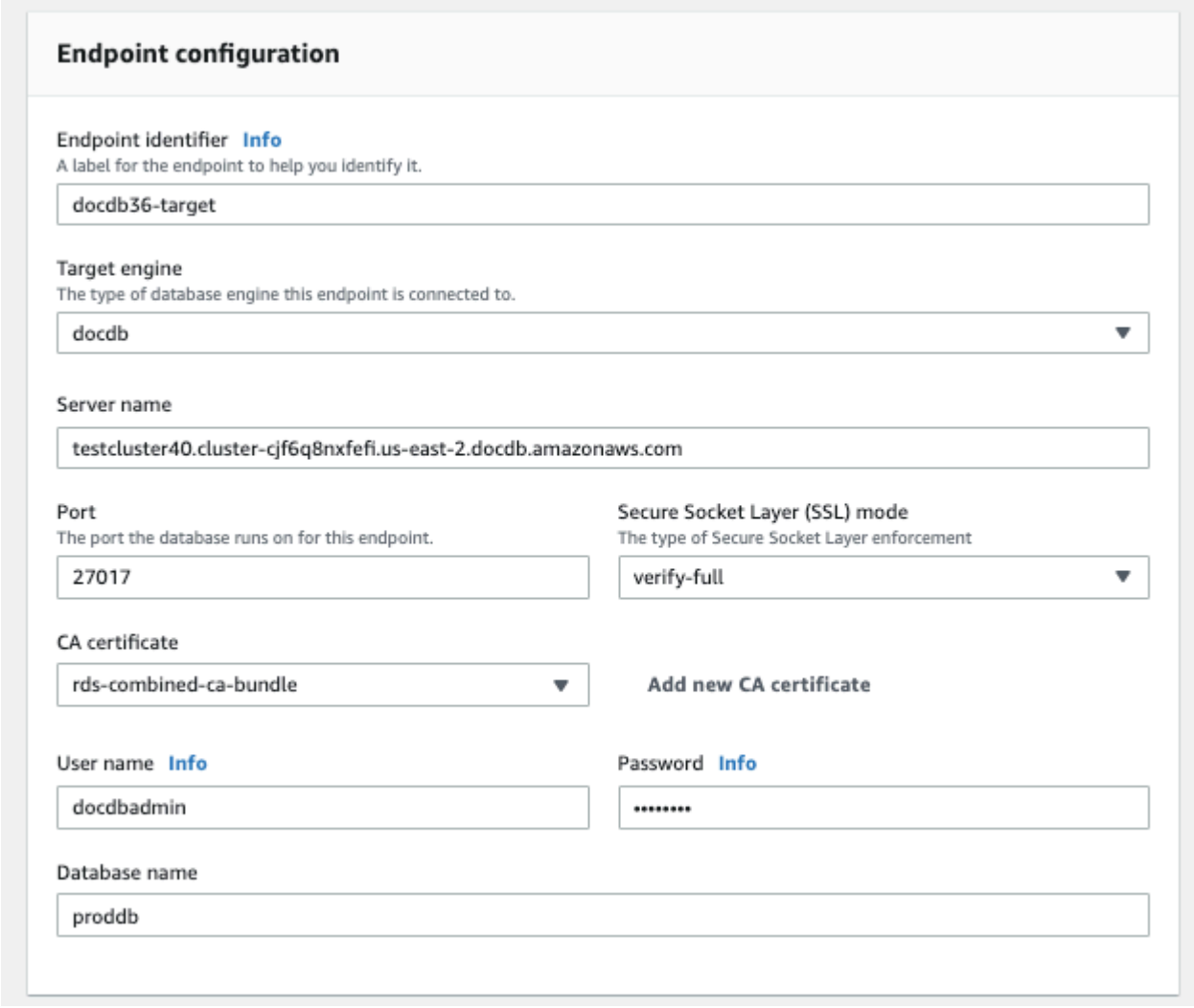
Paso 6: Crear un punto final AWS DMS de destino

El punto de conexión de destino es para su clúster de Amazon DocumentDB de destino.

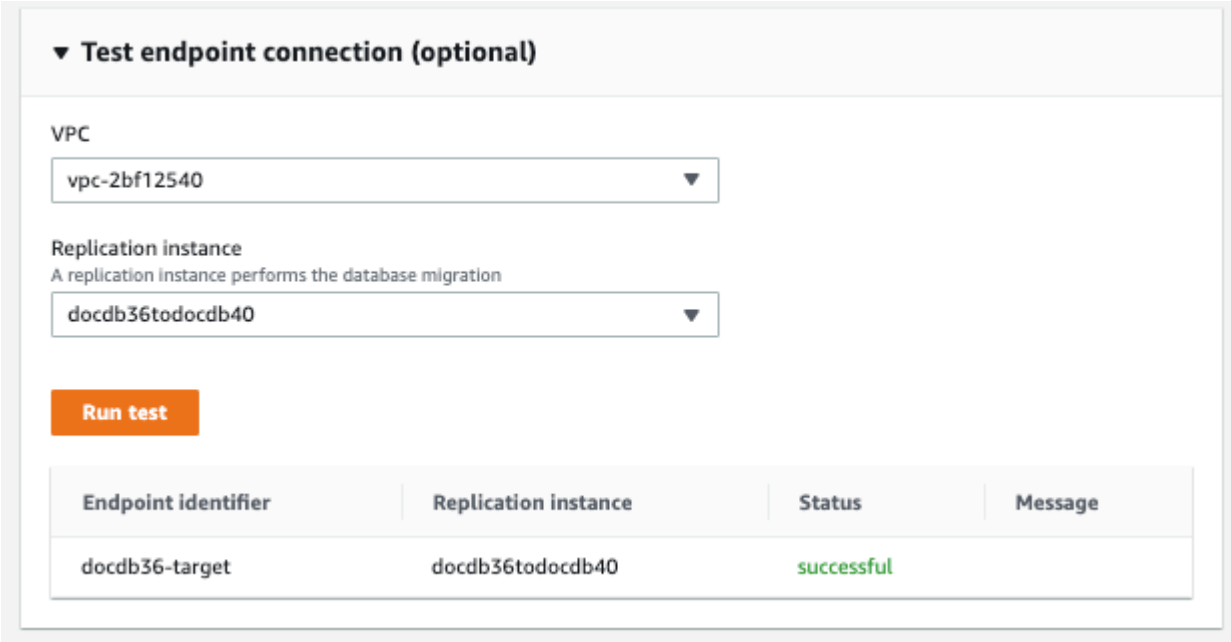
Para crear un punto de conexión de destino:

1. Abra la consola de AWS DMS.
2. En el panel de navegación, elija Puntos de conexión.
3. Elija Create endpoint (Crear punto de conexión) y escriba la siguiente información:
   - En Endpoint Type (Tipo de punto de conexión), elija Target (Destino).
   - En Endpoint identifier (identificador de punto de conexión), escriba un nombre que sea fácil de recordar, como `docdb-target`.
   - En Motor de origen, seleccione `docdb`.
   - En Nombre de servidor, escriba el nombre DNS de su clúster de Amazon DocumentDB de destino.

- En Puerto, escriba el número de puerto de su clúster de Amazon DocumentDB de destino.
- En Modo de SSL, elija `verify-full`.
- En Certificado de CA, elija el `rds-combined-ca-bundle` certificado existente en el menú desplegable Elija un certificado.
- En Nombre de usuario, escriba el nombre de usuario principal del clúster de Amazon DocumentDB de destino.
- En Contraseña, escriba la contraseña principal del clúster de Amazon DocumentDB de destino.
- En Nombre de la base de datos, introduzca el mismo nombre de base de datos que utilizó para configurar el punto de conexión de origen.



4. Pruebe la conexión para comprobar que se configuró correctamente.



5. Elija Create Endpoint (Crear punto de conexión).

Paso 7: crear y ejecutar una tarea de migración

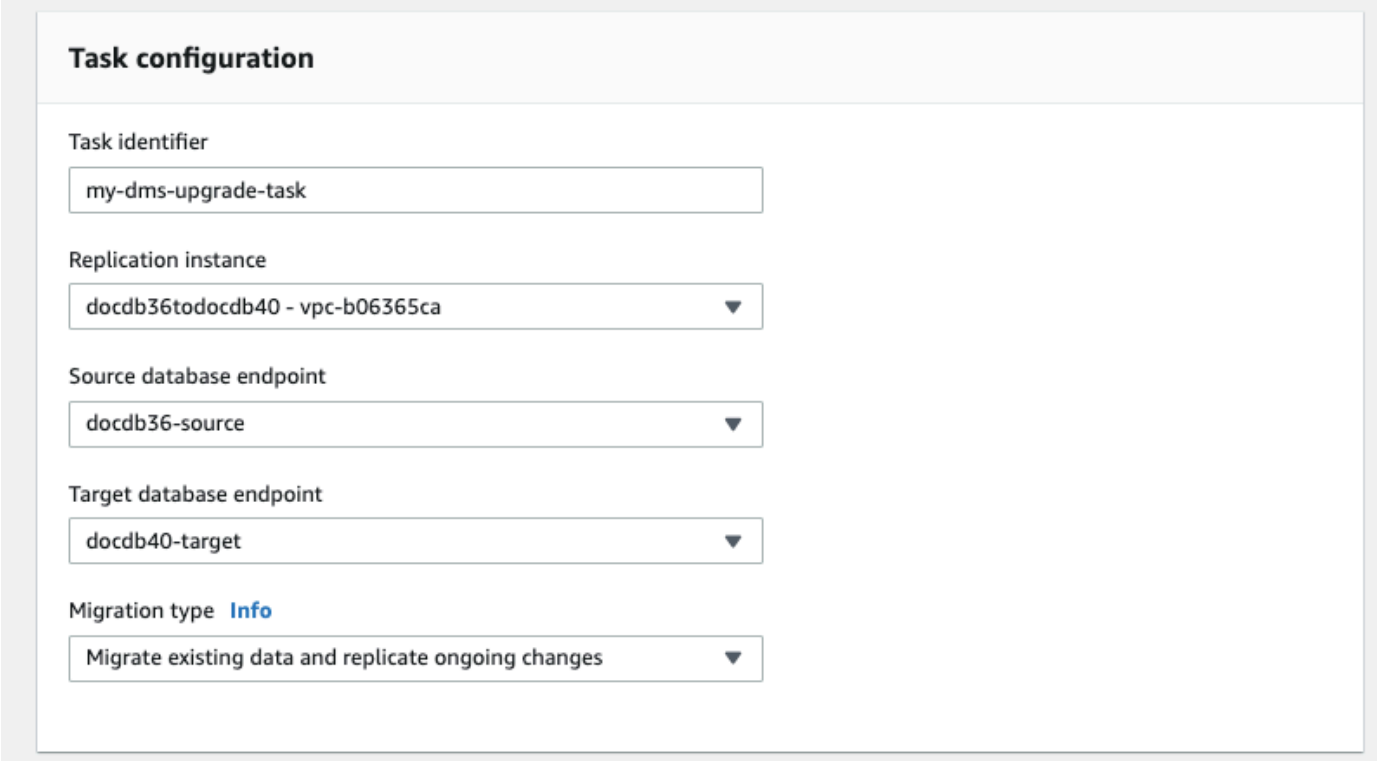
Una AWS DMS tarea vincula la instancia de replicación con la instancia de origen y la de destino. Al crear una tarea de migración, especifique el punto de conexión de origen, el punto de conexión de destino y la instancia de replicación, junto con cualquier configuración de migración deseada. Se puede crear una AWS DMS tarea con tres tipos de migración diferentes: migrar los datos existentes, migrar los datos existentes y replicar los cambios en curso o replicar únicamente los cambios en los datos. Debido a que el objetivo de este tutorial es actualizar un clúster de Amazon DocumentDB con un tiempo de inactividad mínimo, los pasos utilizan la opción de migrar los datos existentes y de replicar los cambios en curso. Con esta opción, AWS DMS captura los cambios mientras migra los datos existentes. AWS DMS sigue capturando y aplicando los cambios incluso después de que se hayan cargado los datos masivos. Con el tiempo, las bases de datos de origen y de destino se sincronizarán, por lo que el tiempo de inactividad de la migración será mínimo.

A continuación, se detallan los pasos para crear una tarea de migración con un tiempo de inactividad mínimo:

1. Abre la AWS DMS consola.
2. En el panel de navegación, elija Tareas de migración de base de datos.

3. Elija Crear tarea de migración de base de datos e introduzca la siguiente información en la sección Configuración de tareas:

   - En Identificador de la tarea, escriba un nombre que sea fácil de recordar, como `my-dms-upgrade-task`.
   - En el Nombre de recurso de Amazon (ARN) descriptivo, introduzca un nombre fácil de usar para anular el ARN de DMS predeterminado.
   - En Replication instance (Instancia de replicación), elija la instancia de replicación que creó en Paso 4: Crear una AWS DMS instancia de replicación.
   - En Punto de conexión de la base de datos de origen, elija el punto de conexión de origen que creó en Paso 5: Crear un punto final AWS DMS de origen.
   - En Punto de conexión de destino, elija el punto de conexión de destino que creó en Paso 6: Crear un punto final AWS DMS de destino.
   - En Tipo de migración, elija Migración y réplica.

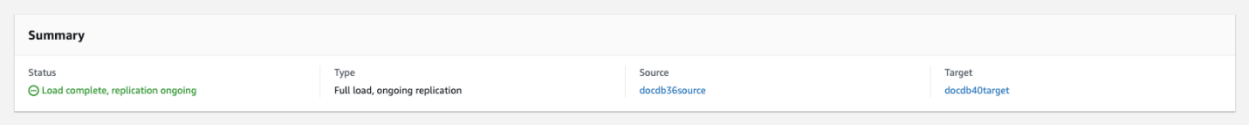


4. Introduzca la siguiente información en la sección Configuración de tareas:

   - En la sección Modo de preparación de la tabla de destino, elija No hacer nada. Esto garantizará que los índices creados en el paso 3 no se eliminen.

- En la subsección Registros de tareas, selecciona Activar CloudWatch registros.
- En Configuración de inicio de la tarea de migración, seleccione Automáticamente con la creación. Esto iniciará la tarea de migración automáticamente una vez que la haya creado.
- Seleccione Crear tarea de migración de bases de datos.

AWS DMS ahora comienza a migrar los datos del clúster de Amazon DocumentDB de origen al clúster de Amazon DocumentDB de destino. El estado de la tarea debe cambiar de Iniciándose a En ejecución. Puede supervisar el progreso seleccionando Tareas en la consola. AWS DMS Después de varias minutes/hours (según el tamaño de la migración), el estado debería cambiar de Carga completa y la replicación en curso. Esto significa que AWS DMS ha completado una migración a carga completa del clúster de Amazon DocumentDB de origen a un clúster de Amazon DocumentDB de destino y ahora está replicando los eventos de cambio.



Finalmente, el origen y el destino se sincronizarán. Para comprobar si están sincronizados, ejecute una operación `count()` en sus colecciones para comprobar que todos los eventos de cambio se hayan migrado.

Paso 8: cambiar el punto de conexión de origen de la aplicación al clúster de Amazon DocumentDB de destino

Cuando se complete la carga completa y el proceso de CDC se replique de forma continua, estará listo para cambiar el punto de conexión de la base de datos de su aplicación del clúster de Amazon DocumentDB de origen al clúster de Amazon DocumentDB de destino.

Soporte extendido de Amazon DocumentDB

El Soporte extendido de Amazon DocumentDB le permite seguir ejecutando una versión del motor después de la fecha de finalización del soporte estándar por un costo adicional. Los clústeres se inscriben en el Soporte extendido una vez finalizada la fecha del soporte estándar. Si no completa las actualizaciones antes de que finalice la fecha de soporte estándar de la versión del motor, los clústeres se facturarán según la tarifa del Soporte extendido.

Temas

- Información general del soporte extendido
- Precios del Soporte extendido
- Responsabilidades

El Soporte extendido de Amazon DocumentDB ofrece las siguientes actualizaciones y soporte técnico:

- Actualizaciones de seguridad para las CVE críticas y altas para la instancia o el clúster
- Correcciones de errores y parches para problemas críticos
- La posibilidad de abrir casos de soporte y recibir ayuda para la solución de problemas según el Acuerdo de nivel de servicio de Amazon DocumentDB.

Esta oferta de pago le da más tiempo para llevar a cabo la actualización a una versión del motor compatible. Por ejemplo, la fecha de finalización del soporte estándar de Amazon DocumentDB para la versión 3.6 es el 30 de marzo de 2026; sin embargo, no está preparado para actualizar a la versión 5.0 antes de esa fecha. En este caso, Amazon DocumentDB inscribe su clúster de la versión 3.6 en el Soporte extendido para que pueda seguir utilizando la versión 3.6 de Amazon DocumentDB. A partir del 31 de marzo de 2026, AWS cobrará una prima por el Soporte extendido para los clústeres de la versión 3.6 de Amazon DocumentDB.

El Soporte extendido de Amazon DocumentDB está disponible durante un máximo de 3 años después de la fecha de finalización del soporte estándar para la versión del motor. Transcurrido este tiempo, si no ha actualizado la versión del motor a una versión compatible, Amazon DocumentDB actualizará la versión del motor. Se recomienda que haga la actualización a una versión del motor compatible lo antes posible.

Fecha de finalización del soporte estándar de la versión 3.6 de Amazon DocumentDB y fechas del Soporte extendido:

- Publicación de la versión 3.6: 9 de enero de 2019
- Finalización del soporte estándar de la versión 3.6: 30 de marzo de 2026
- Inicio del Soporte extendido de la versión 3.6 (precio del primer año): 31 de marzo de 2026
- Inicio del Soporte extendido de la versión 3.6 (precio del tercer año): 31 de marzo de 2028
- Finalización del Soporte extendido de la versión 3.6: 30 de marzo de 2029

Información general del soporte extendido

Amazon DocumentDB actualiza el clúster a la última versión del motor publicada (antes de que finalice la fecha del Soporte extendido), si el clúster aún no está en esa versión. El período de actualización no tendrá lugar hasta después de la fecha de soporte estándar para esa versión del motor.

Puede crear nuevos clústeres con una versión del motor que haya alcanzado la fecha de finalización del soporte estándar, si ya tiene un clúster en esa versión del motor. Amazon DocumentDB inscribe estos nuevos clústeres en el Soporte extendido de Amazon DocumentDB y le cobra por esta oferta. Si actualiza a una versión del motor que aún se encuentra recibiendo el soporte estándar de Amazon DocumentDB antes de la fecha de finalización del soporte estándar de la versión 3.6, no se le cobrará la prima del Soporte extendido.

Puede finalizar la inscripción en el Soporte extendido de Amazon DocumentDB en cualquier momento. Para finalizar la inscripción, actualice cada clúster inscrito a una versión de motor más reciente cuyo soporte estándar de Amazon DocumentDB siga vigente. La finalización de la inscripción en el Soporte extendido de Amazon DocumentDB entrará en vigor el día en que complete una actualización a una versión más reciente del motor cuyo soporte estándar de Amazon DocumentDB siga vigente.

Para obtener más información sobre las fechas de finalización del soporte estándar de Amazon DocumentDB y las fechas de finalización del Soporte extendido de Amazon DocumentDB, consulte Fechas de soporte de la versión del motor de Amazon DocumentDB.

Precios del Soporte extendido

Incurrirá en cargos por todos los clústeres que se ejecuten en el Soporte extendido a partir del día siguiente a la fecha de finalización del soporte estándar de la versión 3.6 de Amazon DocumentDB. Para conocer la fecha de finalización del soporte estándar de la versión 3.6 de Amazon DocumentDB, consulte Fechas de soporte de la versión del motor de Amazon DocumentDB.

El cargo adicional del Soporte extendido de Amazon DocumentDB se detiene cuando realiza una de las siguientes acciones:

- Actualiza a una versión de motor incluida en el soporte estándar.
- Elimina el clúster que se ejecuta en la versión 3.6 pasada la fecha de finalización del soporte estándar.

Por ejemplo, la versión 3.6 de Amazon DocumentDB entrará en el Soporte extendido el 30 de marzo de 2026, pero los cargos no comenzarán hasta el 31 de marzo de 2026. Si actualiza su clúster de la versión 3.6 de Amazon DocumentDB a la versión 5.0 Amazon DocumentDB el 29 de abril de 2026, se le cobrarán solamente 30 días del Soporte extendido para la versión 3.6 de Amazon DocumentDB. Para obtener más información, consulte Precios de Amazon DocumentDB.

Responsabilidades

Las siguientes son las responsabilidades de Amazon DocumentDB y sus responsabilidades en relación con el Soporte extendido de Amazon DocumentDB.

Responsabilidades de Amazon DocumentDB

Tras la fecha de finalización del soporte estándar de la versión 3.6 de Amazon DocumentDB, Amazon DocumentDB aplicará parches, correcciones de errores y actualizaciones a los clústeres de la versión 3.6 inscritos en el Soporte extendido.

Sus responsabilidades

Usted es responsable de actualizar el motor a una versión más reciente antes de la fecha de finalización del Soporte extendido de la versión 3.6 de Amazon DocumentDB. Si no actualiza el clúster, después de la fecha de finalización del Soporte extendido de la versión 3.6 de Amazon DocumentDB, este intentará actualizar el clúster a la última versión del motor con soporte estándar de Amazon DocumentDB.

Seguridad en Amazon DocumentDB

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de un centro de datos y una arquitectura de red diseñados para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre usted AWS y usted. Esta documentación le permite comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza Amazon DocumentDB. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la AWS nube. AWS también le proporciona servicios que puede utilizar de forma segura. Auditores independientes prueban y verifican periódicamente la eficacia de nuestra seguridad en el marco de los programas de conformidad de AWS. Para obtener más información acerca de los programas de conformidad que se aplican a Amazon DocumentDB (con compatibilidad con MongoDB), consulte Servicios de AWS en el ámbito del programa de conformidad.
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. Usted también es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

Amazon DocumentDB está autorizada por el Programa federal de administración de riesgos y autorizaciones (FedRAMP). Cuenta con una autorización alta de FedRAMP AWS GovCloud para las regiones (EE. UU.) y una autorización moderada de FedRAMP para las regiones de EE. UU. AWS East/West Para obtener información detallada AWS y sobre las iniciativas de cumplimiento, consulte los AWS servicios incluidos en el ámbito de aplicación por programa de cumplimiento.

> **Note**
>
> Este capítulo se aplica a clústeres basados en instancias y clústeres elásticos. Para obtener más información, consulte los siguientes temas.

También aprenderá a utilizar otros AWS servicios que le ayudan a supervisar y proteger sus recursos de Amazon DocumentDB. En los siguientes temas, se mostrará cómo configurar Amazon DocumentDB para satisfacer sus objetivos de seguridad y conformidad.

Temas

- Administración de contraseñas con Amazon DocumentDB y AWS Secrets Manager
- Protección de datos en Amazon DocumentDB
- Identity and Access Management para Amazon DocumentDB
- Autenticación mediante la identidad de IAM
- Administración de usuarios de Amazon DocumentDB
- Acceso a la base de datos mediante el control de acceso basado en roles
- Registro y supervisión en Amazon DocumentDB
- Actualización de los certificados TLS de Amazon DocumentDB
- Actualización de los certificados TLS de Amazon DocumentDB: GovCloud
- Validación de la conformidad en Amazon DocumentDB
- Resiliencia de Amazon DocumentDB
- Seguridad de la infraestructura en Amazon DocumentDB
- API de Amazon DocumentDB y puntos de conexión de VPC de interfaz (AWS PrivateLink)
- Prácticas recomendadas de seguridad para Amazon DocumentDB
- Auditoría de eventos de Amazon DocumentDB
- Amazon VPC y Amazon DocumentDB

Administración de contraseñas con Amazon DocumentDB y AWS Secrets Manager

Amazon DocumentDB se integra con Secrets Manager para administrar las contraseñas de los usuarios principales de los clústeres.

Temas

- Limitaciones de la integración de Secrets Manager con Amazon DocumentDB
- Descripción general de la administración de las contraseñas de los usuarios principales con AWS Secrets Manager
- Hacer cumplir la administración de Amazon DocumentDB de la contraseña del usuario principal en AWS Secrets Manager
- Administración de la contraseña del usuario principal para un clúster con Secrets Manager

Limitaciones de la integración de Secrets Manager con Amazon DocumentDB

Las siguientes características no admiten la administración de contraseñas del usuario principal con Secrets Manager:

- Clústeres que forman parte de una base de datos global de Amazon DocumentDB.
- Réplicas de lectura de Amazon DocumentDB para diferentes regiones.

Descripción general de la administración de las contraseñas de los usuarios principales con AWS Secrets Manager

Con AWS Secrets Manager, puedes reemplazar las credenciales codificadas de tu código, incluidas las contraseñas de las bases de datos, por una llamada a la API a Secrets Manager para recuperar el secreto mediante programación. Para obtener más información acerca de Secrets Manager, consulte la Guía del usuario de AWS Secrets Manager.

Cuando guardas secretos de bases de datos en Secrets Manager, tu AWS cuenta incurre en cargos. Para obtener información sobre precios, consulte Precios de AWS Secrets Manager.

Puede especificar que Amazon DocumentDB administre la contraseña de usuario principal en Secrets Manager para un clúster de Amazon DocumentDB cuando realice una de las siguientes operaciones:

- Cree el clúster
- Modificación del clúster

Cuando especifica que Amazon DocumentDB administre la contraseña del usuario principal en Secrets Manager, Amazon DocumentDB genera la contraseña y la almacena en Secrets Manager. Puede interactuar directamente con el secreto para recuperar las credenciales del usuario principal. También puede especificar una clave gestionada por el cliente para cifrar el secreto o utilizar la clave de KMS que proporciona Secrets Manager.

Amazon DocumentDB administra la configuración del secreto y lo rota cada siete días de forma predeterminada. Puede modificar algunos de los ajustes, como el programa de rotación. Si elimina un clúster que administra un secreto en Secrets Manager, también se eliminarán el secreto y sus metadatos asociados.

Para conectarse a un clúster con las credenciales en un secreto, puede recuperar el secreto en Secrets Manager. Para obtener más información, consulte Obtener secretos de una base de datos SQL AWS Secrets Manager y conectarse a ella mediante JDBC con credenciales en AWS Secrets Manager secreto en la Guía del AWS Secrets Manager usuario.

Hacer cumplir la administración de Amazon DocumentDB de la contraseña del usuario principal en AWS Secrets Manager

Puede utilizar las claves de condición de IAM para hacer que Amazon DocumentDB administre la contraseña del usuario principal en AWS Secrets Manager. La siguiente política no permite que los usuarios creen ni restauren instancias ni clústeres a menos que Amazon DocumentDB administre la contraseña del usuario principal en Secrets Manager.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "rds:CreateDBCluster"
            ],
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "rds:ManageMasterUserPassword": false
                }
            }
        }
    ]
}
```

Administración de la contraseña del usuario principal para un clúster con Secrets Manager

Para configurar la administración de Amazon DocumentDB de la contraseña del usuario principal en Secrets Manager, debe realizar las siguientes acciones:

- Creación de un clúster de Amazon DocumentDB
- Modificación de un clúster de Amazon DocumentDB

Puede utilizar la consola Amazon DocumentDB o la AWS CLI para realizar estas acciones.

Protección de datos en Amazon DocumentDB

El modelo de responsabilidad compartida de AWS se aplica a la protección de los datos en Amazon DocumentDB (compatible con MongoDB). Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta toda la Nube de AWS. Eres responsable de mantener el control sobre el contenido alojado en esta infraestructura. También eres responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulta las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulta la publicación de blog sobre el Modelo de responsabilidad compartida de AWS y GDPR en el Blog de seguridad de AWS.

Con fines de protección de datos, recomendamos proteger las credenciales de la Cuenta de AWS y configurar cuentas de usuario individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utiliza la autenticación multifactor (MFA) en cada cuenta.
- Utiliza SSL/TLS para comunicarse con los recursos de AWS. Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure los registros de API y de actividad de los usuarios con AWS CloudTrail. Para obtener información sobre cómo utilizar registros de seguimiento de CloudTrail para capturar actividades de AWS, consulta Working with CloudTrail trails en la Guía del usuario de AWS CloudTrail.
- Utiliza las soluciones de cifrado de AWS, junto con todos los controles de seguridad predeterminados dentro de los servicios de Servicios de AWS.
- Utiliza servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados FIPS 140-3 al acceder a AWS a través de una interfaz de línea de comandos o una API, utiliza un punto de conexión de FIPS. Para obtener

más información sobre los puntos de conexión de FIPS disponibles, consulta Estándar de procesamiento de la información federal (FIPS) 140-3.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabaja con Amazon DocumentDB u otros Servicios de AWS mediante la consola, la API, la AWS CLI o los SDK de AWS. Cualquier dato que ingrese en etiquetas o campos de texto de formato libre utilizados para nombres se puede emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

Temas

- Cifrado a nivel de campo del lado del cliente
- Cifrado de datos en reposo de Amazon DocumentDB
- Cifrado de datos en tránsito
- Administración de claves

Cifrado a nivel de campo del lado del cliente

El cifrado a nivel de campo (FLE) del lado del cliente de Amazon DocumentDB le permite cifrar los datos confidenciales de las aplicaciones cliente antes de transferirlos a un clúster de Amazon DocumentDB. Los datos confidenciales permanecen cifrados cuando se almacenan y procesan en un clúster y se descifran en la aplicación cliente cuando se recuperan.

Temas

- Introducción
- Consultas en el FLE del lado del cliente
- Limitaciones

Introducción

La configuración inicial del FLE del lado del cliente en Amazon DocumentDB es un proceso de cuatro pasos que incluye la creación de una clave de cifrado, la asociación de un rol a la aplicación, la configuración de la aplicación y la definición de la operación CRUD con las opciones de cifrado.

Temas

- Paso 1: crear las claves de cifrado
- Paso 2: asociar un rol a la aplicación
- Paso 3: configurar la aplicación
- Paso 4: definir una operación CRUD
- Ejemplo: archivo de configuración de cifrado a nivel de campo del lado del cliente

Paso 1: crear las claves de cifrado

Con AWS Key Management Service, cree una clave simétrica que se utilice para cifrar y descifrar el campo de datos confidenciales y asígnele los permisos de uso de IAM necesarios. AWS KMS almacena la clave de cliente (CK) que se utiliza para cifrar las claves de datos (DK). Recomendamos almacenar la clave de cliente en KMS para reforzar su postura de seguridad. La clave de datos es la clave secundaria que se almacena en una colección de Amazon DocumentDB y se requiere para cifrar los campos confidenciales antes de almacenar el documento en Amazon DocumentDB. La clave de cliente cifra la clave de datos, que a su vez cifra y descifra sus datos. Si utiliza un clúster global, puede crear una clave multirregional que puedan utilizar distintos roles de servicio en distintas regiones.

Para obtener más información sobre la AWS Key Management Service, incluida la forma de crearla, consulte la Guía para desarrolladores del Servicio de administración de claves de AWS.

Paso 2: asociar un rol a la aplicación

Crear una política de IAM con permisos de AWS KMS apropiados. Esta política permite a las identidades de IAM a las que está asociada obtener y descifrar la clave KMS especificada en el campo de recursos. La aplicación asume este rol de IAM para autenticarse con AWS KMS.

El aspecto de la respuesta debe ser parecido al siguiente:

```
{ "Effect": "Allow",
"Action": ["kms:Decrypt", "kms:Encrypt"],
"Resource": "Customer Key ARN"
}
```

Paso 3: configurar la aplicación

A estas alturas, ya ha definido una clave de cliente en AWS KMS, ha creado una función de rol de IAM y le ha otorgado los permisos de IAM correctos para acceder a la clave de cliente. Importe estos paquetes necesarios.

```
import boto3
import json
import base64
from pymongo import MongoClient
from pymongo.encryption import (Algorithm,
                                ClientEncryption)
```

```
# create a session object:
my_session = boto3.session.Session()

# get access_key and secret_key programmatically using get_frozen_credentials() method:
 current_credentials = my_session.get_credentials().get_frozen_credentials()
```

1. Especifique “aws” como tipo de proveedor de KMS e introduzca las credenciales de su cuenta, que se recuperaron en el paso anterior.

   ```
   provider = "aws"
   kms_providers = {
       provider: {
           "accessKeyId": current_credentials.access_key,
           "secretAccessKey": current_credentials.secret_key
       }
   }
   ```

2. Especifique la clave del cliente que se utiliza para cifrar la clave de datos:

   ```
   customer_key = {
   “region”: “AWS region of the customer_key”,
       “key”: “customer_key ARN”
   }

   key_vault_namespace = "encryption.dataKeys"

   key_alt_name = 'TEST_DATA_KEY'
   ```

3. Configure el objeto MongoClient:

```
client = MongoClient(connection_string)

coll = client.test.coll
coll.drop()

client_encryption = ClientEncryption(
    kms_providers, # pass in the kms_providers variable from the previous step
    key_vault_namespace = key_vault_namespace,
    client,
    coll.codec_options
)
```

4. Genere su clave de datos:

```
data_key_id = client_encryption.create_data_key(provider,
    customer_key,
    key_alt_name = [key_alt_name])
```

5. Recupera tu clave de datos existente:

```
data_key = DataKey("aws",
    master_key = customer_key)
key_id = data_key["_id"]
data_key_id = client[key_vault_namespace].find_one({"_id": key_id})
```

Paso 4: definir una operación CRUD

Defina la operación CRUD con opciones de cifrado.

1. Defina la colección para escribir/leer/eliminar un solo documento:

```
coll = client.gameinfo.users
```

2. Cifrado explícito: cifra los campos e inserta:

> **Note**
>
> Debe proporcionarse exactamente uno de los siguientes valores: “key_id” o “key_alt_name”.

```
encrypted_first_name = client_encryption.encrypt(
    "Jane",
    Algorithm.AEAD_AES_256_CBC_HMAC_SHA_512_Deterministic,
    key_alt_name=data_key_id
)
encrypted_last_name = client_encryption.encrypt(
    "Doe",
    Algorithm.AEAD_AES_256_CBC_HMAC_SHA_512_Deterministic,
    key_alt_name=data_key_id
)
encrypted_dob = client_encryption.encrypt(
    "1990-01-01",
    Algorithm.AEAD_AES_256_CBC_HMAC_SHA_512_Random,
    key_alt_name=data_key_id
)

coll.insert_one(
    {"gamerTag": "jane_doe90",
    "firstName": encrypted_first_name,
    "lastName": encrypted_last_name,
    "dateOfBirth":encrypted_dob,
    "Favorite_games":["Halo","Age of Empires 2","Medal of Honor"]
})
```

Ejemplo: archivo de configuración de cifrado a nivel de campo del lado del cliente

En el siguiente ejemplo, reemplace cada *`marcador de posición del usuario`* con su propia información.

```
# import python packages:
import boto3
import json
import base64
from pymongo import MongoClient
from pymongo.encryption import (Algorithm,
                                ClientEncryption)

def main():

    # create a session object:
```

```
    my_session = boto3.session.Session()

    # get aws_region from session object:
    aws_region = my_session.region_name

    # get access_key and secret_key programmatically using get_frozen_credentials()
 method:
    current_credentials = my_session.get_credentials().get_frozen_credentials()
    provider = "aws"

    # define the kms_providers which is later used to create the Data Key:
    kms_providers = {
        provider: {
            "accessKeyId": current_credentials.access_key,
            "secretAccessKey": current_credentials.secret_key
        }
    }

    # enter the kms key ARN. Replace the example ARN value.
    kms_arn = "arn:aws:kms:us-east-1:123456789:key/abcd-efgh-ijkl-mnop"
    customer_key = {
        "region": aws_region,
        "key":kms_arn
    }

    # secrets manager is used to strore and retrieve user credentials for connecting to
 an Amazon DocumentDB cluster.
    # retrieve the secret using the secret name. Replace the example secret key.
    secret_name = "/dev/secretKey"
    docdb_credentials = json.loads(my_session.client(service_name = 'secretsmanager',
 region_name = "us-east-1").get_secret_value(SecretId = secret_name)['SecretString'])

    connection_params = '/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false'
    conn_str = 'mongodb://' + docdb_credentials["username"] + ':' +
 docdb_credentials["password"] + '@' + docdb_credentials["host"] + ':' +
 str(docdb_credentials["port"]) + connection_params
    client = MongoClient(conn_str)

    coll = client.test.coll
    coll.drop()

    # store the encryption data keys in a key vault collection (having naming
 convention as db.collection):
```

```
    key_vault_namespace = "encryption.dataKeys"
    key_vault_db_name, key_vault_coll_name = key_vault_namespace.split(".", 1)

    # set up the key vault (key_vault_namespace) for this example:
    key_vault = client[key_vault_db_name][key_vault_coll_name]
    key_vault.drop()
    key_vault.create_index("keyAltNames", unique=True)

    client_encryption = ClientEncryption(
        kms_providers,
        key_vault_namespace,
        client,
        coll.codec_options)

    # create a new data key for the encrypted field:
    data_key_id = client_encryption.create_data_key(provider, master_key=customer_key,
key_alt_names=["some_key_alt_name"], key_material = None)

    # explicitly encrypt a field:
    encrypted_first_name = client_encryption.encrypt(
    "Jane",
    Algorithm.AEAD_AES_256_CBC_HMAC_SHA_512_Deterministic,
    key_id=data_key_id
    )
    coll.insert_one(
    {"gamerTag": "jane_doe90",
    "firstName": encrypted_first_name
    })
    doc = coll.find_one()
    print('Encrypted document: %s' % (doc,))

    # explicitly decrypt the field:
    doc["encryptedField"] = client_encryption.decrypt(doc["encryptedField"])
    print('Decrypted document: %s' % (doc,))

    # cleanup resources:
    client_encryption.close()
    client.close()

    if __name__ == "__main__":
        main()
```

Consultas en el FLE del lado del cliente

Amazon DocumentDB admite consultas de igualdad de puntos con FLE del lado del cliente. Las consultas de desigualdad y comparación pueden arrojar resultados imprecisos. Las operaciones de lectura y escritura pueden tener un comportamiento inesperado o incorrecto en comparación con ejecutar la misma operación con el valor descifrado.

Por ejemplo, para consultar los filtros de documentos con una puntuación de jugador superior a 500:

```
db.users.find( {
    "gamerscore" : { $gt : 500 }
})
```

El cliente utiliza un método de cifrado explícito para cifrar el valor de la consulta:

```
encrypted_gamerscore_filter = client_encryption.encrypt(
    500,
        Algorithm.AEAD_AES_256_CBC_HMAC_SHA_512_Deterministic,
        key_alt_name=data_key_id
        )

db.users.find( {
    "gamerscore" : { $gt : encrypted_gamerscore_filter }
} )
```

En la operación de búsqueda, Amazon DocumentDB compara el valor cifrado de 500 con los valores de campo cifrados almacenados en cada documento mediante la comprobación superior a la desigualdad. La comprobación de desigualdad de la operación de búsqueda puede arrojar un resultado diferente si se realiza con datos y valores descifrados, aunque la operación genere resultados satisfactoriamente.

Limitaciones

Las siguientes limitaciones se aplican al cifrado a nivel de campo del lado del cliente de Amazon DocumentDB:

- Amazon DocumentDB solo admite consultas de igualdad de puntos. Las consultas de desigualdad y comparación pueden arrojar resultados imprecisos. Las operaciones de lectura y escritura pueden tener un comportamiento inesperado o incorrecto en comparación con ejecutar la misma operación con el valor descifrado. Para consultar los filtros de documentos con una puntuación de jugador superior a 500.

```
db.users.find( {
    "gamerscore" : { $gt : 500 }
    })
```

El cliente utiliza un método de cifrado explícito para cifrar el valor de la consulta.

```
encrypted_gamerscore_filter = client_encryption.encrypt(
    500,
    Algorithm.AEAD_AES_256_CBC_HMAC_SHA_512_Deterministic,
    key_alt_name=data_key_id
)

db.users.find({
    "gamerscore" : { $gt : encrypted_gamerscore_filter }
})
```

En la operación de búsqueda, Amazon DocumentDB compara el valor cifrado de 500 con los valores de campo cifrados almacenados en cada documento mediante la comprobación superior a la desigualdad. La comprobación de desigualdad de la operación de búsqueda puede arrojar un resultado diferente si se realiza con datos y valores descifrados, aunque la operación genere resultados satisfactoriamente.

- Amazon DocumentDB no admite el FLE explícito del lado del cliente desde el intérprete de comandos Mongo. Sin embargo, la característica funciona con cualquiera de nuestros controladores compatibles.

Cifrado de datos en reposo de Amazon DocumentDB

> **Note**
>
> AWS KMS está reemplazando el término clave maestra del cliente (CMK) por AWS KMS key y Clave KMS. El concepto no ha cambiado. Para evitar que se produzcan cambios bruscos, AWS KMS está manteniendo algunas variaciones de este término.

Puede cifrar los datos en reposo del clúster de Amazon DocumentDB especificando la opción de cifrado de almacenamiento al crear el clúster. El cifrado de almacenamiento está habilitado para todo el clúster y se aplica a todas las instancias, incluida la instancia principal y las réplicas. También se

aplica al volumen de almacenamiento, los datos, los índices, los registros, las copias de seguridad automatizadas y las instantáneas del clúster.

Amazon DocumentDB utiliza el estándar de cifrado avanzado de 256 bits (AES-256) para cifrar sus datos mediante claves de cifrado almacenadas en AWS Key Management Service (AWS KMS). Si utiliza un clúster de Amazon DocumentDB con el cifrado en reposo activado, no necesita modificar la lógica de la aplicación ni la conexión del cliente. Amazon DocumentDB se encarga del cifrado y descifrado de sus datos de forma transparente con un impacto mínimo en el desempeño.

Amazon DocumentDB se integra con AWS KMS y utiliza un método conocido como cifrado de sobre para proteger sus datos. Cuando un clúster de Amazon DocumentDB se cifra con unAWS KMS, Amazon DocumentDB le pide AWS KMS que utilice su clave de KMS para generar una clave de datos de texto cifrado para cifrar el volumen de almacenamiento. La clave de datos de texto cifrado se cifra mediante la clave KMS que ha definido y se almacena junto con los datos cifrados y los metadatos de almacenamiento. Cuando Amazon DocumentDB necesita acceder a los datos cifrados, solicita a AWS KMS que descifre la clave de datos de texto cifrado utilizando su clave KMS y almacena en la memoria caché la clave de datos de texto sin formato con el fin de cifrar y descifrar de manera eficiente los datos en el volumen de almacenamiento.

La función de cifrado de almacenamiento de Amazon DocumentDB está disponible para todos los tamaños de instancias y en todas las Regiones de AWS en las que Amazon DocumentDB está disponible.

Habilitación del cifrado en reposo de un clúster de Amazon DocumentDB

Puede habilitar o deshabilitar el cifrado en reposo en un clúster de Amazon DocumentDB cuando el clúster se aprovisiona mediante la Consola de administración de AWS o la AWS Command Line Interface (AWS CLI). Los clústeres creados con la consola tienen el cifrado en reposo habilitado de forma predeterminada. Los clústeres creados con la AWS CLI tienen el cifrado en reposo deshabilitado de forma predeterminada. Por lo tanto, debe habilitar explícitamente el cifrado en reposo mediante el `--storage-encrypted` parámetro. En cualquier caso, una vez creado el clúster, no puede cambiar la opción de cifrado en reposo.

Amazon DocumentDB utiliza AWS KMS para recuperar y administrar claves de cifrado y para definir las políticas que controlan cómo se pueden utilizar estas claves. Si no especifica un identificador de clave AWS KMS, Amazon DocumentDB utiliza la clave KMS de AWS de servicio administrado predeterminado. Amazon DocumentDB crea una clave KMS independiente para cada Región de AWS de su Cuenta de AWS. Para obtener más información, consulte Conceptos de AWS Key Management Service.

Para comenzar a crear su propia KMS, consulte Introducción en la AWS Key Management ServiceGuía del desarrollador.

> **Important**
>
> Debe utilizar una clave de cifrado de KMS simétrica para cifrar el clúster, ya que Amazon DocumentDB solo admite claves de cifrado de KMS de cifrado simétricas. No utilice una KMS asimétrica para intentar cifrar los datos de los clústeres de Amazon DocumentDB. Para obtener más información, consulte claves asimétricas de AWS KMS en la Guía para desarrolladores de AWS Key Management Service.

Si Amazon DocumentDB ya no puede obtener acceso a la clave de cifrado de un clúster, por ejemplo, cuando se revoca el acceso a una clave, el clúster cifrado entra en un estado terminal. En este caso, solo puede restaurar el clúster desde una copia de seguridad. Para Amazon DocumentDB, las copias de seguridad siempre están habilitadas durante 1 día.

Además, si deshabilita la clave de un clúster cifrado de Amazon DocumentDB, eventualmente perderá el acceso de lectura y escritura a ese clúster. Cuando Amazon DocumentDB encuentra una instancia que está cifrada con una clave a la que no tiene acceso, pone el clúster en un estado terminal. En dicho estado, el clúster ya no está disponible y no es posible recuperar su estado actual. Para restaurar el clúster, debe volver a activar el acceso a la clave de cifrado para Amazon DocumentDB y después restaurar el clúster a partir de una copia de seguridad.

> **Important**
>
> No puede cambiar la clave KMS de un clúster cifrado después de haberlo creado. Asegúrese de determinar los requisitos de clave de cifrado antes de crear el clúster cifrado.

Using the Consola de administración de AWS

Debe especificar la opción de cifrado en reposo al crear un clúster. El cifrado en reposo se habilita de forma predeterminada cuando se crea un clúster mediante la Consola de administración de AWS. No se puede cambiar una vez creado el clúster.

Para especificar la opción de cifrado en reposo, al crear el clúster

1. Cree un clúster de Amazon DocumentDB como se describe en la sección Introducción. Sin embargo, en el paso 6, no elija Create cluster (Crear clúster).
2. Debajo de la sección Authentication (Autenticación), elija Show advanced settings (Mostrar configuración avanzada).
3. Desplácese hacia abajo hasta la sección Encryption-at-rest (Cifrado en reposo).
4. Elija la opción que desee para el cifrado en reposo. Cualquiera que sea la opción que elija, no podrá cambiarla después de crear el clúster.
   - Para cifrar datos en reposo en este clúster, elija Enable encryption (Habilitar cifrado).
   - Si no desea cifrar datos en reposo en este clúster, elija Disable encryption (Deshabilitar cifrado).
5. Elija la clave principal que desee. Amazon DocumentDB utiliza AWS Key Management Service (AWS KMS) para recuperar y administrar claves de cifrado y para definir las políticas que controlan cómo se pueden utilizar estas claves. Si no especifica un identificador de clave AWS KMS, Amazon DocumentDB utiliza la clave KMS de AWS de servicio administrado predeterminado. Para obtener más información, consulte Conceptos de AWS Key Management Service.

   > **Note**
   >
   > Después de crear un clúster cifrado, no puede cambiar la clave KMS de dicho clúster. Asegúrese de determinar los requisitos de clave de cifrado antes de crear el clúster cifrado.

6. Rellene las demás secciones según sea necesario y cree el clúster.

Using the AWS CLI

Para cifrar un clúster de Amazon DocumentDB mediante la AWS CLI, ejecute el comando `create-db-cluster` y especifique la opción `--storage-encrypted`. Los clústeres de Amazon DocumentDB creados con la AWS CLI no habilitan el cifrado de almacenamiento de forma predeterminada.

En el siguiente ejemplo se crea un clúster de Amazon DocumentDB con el cifrado de almacenamiento habilitado.

En los siguientes ejemplos, reemplace cada *marcador de posición del usuario* con la información de su clúster.

Example

Para Linux, macOS o Unix:

```
aws docdb create-db-cluster \
  --db-cluster-identifier mydocdbcluster \
  --port 27017 \
  --engine docdb \
  --master-username SampleUser1 \
  --master-user-password primaryPassword \
  --storage-encrypted
```

Para Windows:

```
aws docdb create-db-cluster ^
  --db-cluster-identifier SampleUser1 ^
  --port 27017 ^
  --engine docdb ^
  --master-username SampleUser1 ^
  --master-user-password primaryPassword ^
  --storage-encrypted
```

Cuando crea un clúster de Amazon DocumentDB cifrado, puede especificar un identificador de clave de AWS KMS, tal y como se muestra en el siguiente ejemplo.

Example

Para Linux, macOS o Unix:

```
aws docdb create-db-cluster \
  --db-cluster-identifier SampleUser1 \
  --port 27017 \
  --engine docdb \
  --master-username primaryUsername \
  --master-user-password yourPrimaryPassword \
  --storage-encrypted \
  --kms-key-id key-arn-or-alias
```

Para Windows:

```
aws docdb create-db-cluster ^
  --db-cluster-identifier SampleUser1 ^
  --port 27017 ^
  --engine docdb ^
  --master-username SampleUser1 ^
  --master-user-password primaryPassword ^
  --storage-encrypted ^
  --kms-key-id key-arn-or-alias
```

> **Note**
>
> Después de crear un clúster cifrado, no puede cambiar la clave KMS de dicho clúster. Asegúrese de determinar los requisitos de clave de cifrado antes de crear el clúster cifrado.

Limitaciones para clústeres cifrados de Amazon DocumentDB

Los clústeres cifrados de Amazon DocumentDB tienen las siguientes limitaciones:

- Solo puede habilitar o deshabilitar el cifrado en reposo para un clúster de Amazon DocumentDB en el momento en que se crea, no después de que el clúster se haya creado. Sin embargo, puede crear una copia cifrada de un clúster sin cifrar creando una instantánea del clúster sin cifrar y, a continuación, restaurando la instantánea sin cifrar como nuevo clúster mientras especifica la opción de cifrado en reposo.

  Para obtener más información, consulte los temas siguientes:

  - Creación de una instantánea manual del clúster
  - Restauración de una instantánea del clúster
  - Copia de instantáneas de clústeres de Amazon DocumentDB
- Los clústeres de Amazon DocumentDB con el cifrado de almacenamiento habilitado no se pueden modificar para deshabilitar el cifrado.
- Todas las instancias, copias de seguridad automatizadas, instantáneas e índices de un clúster de Amazon DocumentDB se cifran con la misma clave KMS.

Cifrado de datos en tránsito

Puede utilizar seguridad de la capa de transporte (TLS) para cifrar la conexión entre su aplicación y un clúster de Amazon DocumentDB. De forma predeterminada, el cifrado en tránsito está habilitado para los clústeres de Amazon DocumentDB recién creados. Opcionalmente se puede deshabilitar cuando se crea el clúster o en un momento posterior. Cuando se habilita el cifrado en tránsito, se requieren conexiones seguras con TLS para conectarse al clúster. Para obtener más información sobre cómo conectarse a Amazon DocumentDB mediante TLS, consulte Conexión mediante programación a Amazon DocumentDB.

Administración de la configuración de TLS del clúster de Amazon DocumentDB

El cifrado en tránsito para un clúster de Amazon DocumentDB se administra mediante el parámetro TLS en un grupo de parámetros de clúster. Puede administrar la configuración de TLS del clúster de Amazon DocumentDB mediante la Consola de administración de AWS o la AWS Command Line Interface (AWS CLI). Consulte las secciones siguientes para obtener información sobre cómo verificar y modificar la configuración actual de TLS.

Using the Consola de administración de AWS

Siga estos pasos para realizar tareas de administración para el cifrado TLS mediante la consola, como identificar grupos de parámetros, verificar el valor de TLS y realizar las modificaciones necesarias.

> **Note**
>
> A menos que lo especifique de manera diferente al crear un clúster, el clúster se crea con el grupo de parámetros de clúster predeterminado. Los parámetros del `default` grupo de parámetros de clúster no se pueden modificar (por ejemplo, `tls` habilitado/deshabilitado). Por lo tanto, si su clúster está utilizando un `default` grupo de parámetros de clúster, debe modificar el clúster para utilizar un grupo de parámetros de clúster no predeterminado. En primer lugar, es posible que tenga que crear un grupo de parámetros de clúster personalizado. Para obtener más información, consulte Creación de grupos de parámetros de clúster de Amazon DocumentDB.

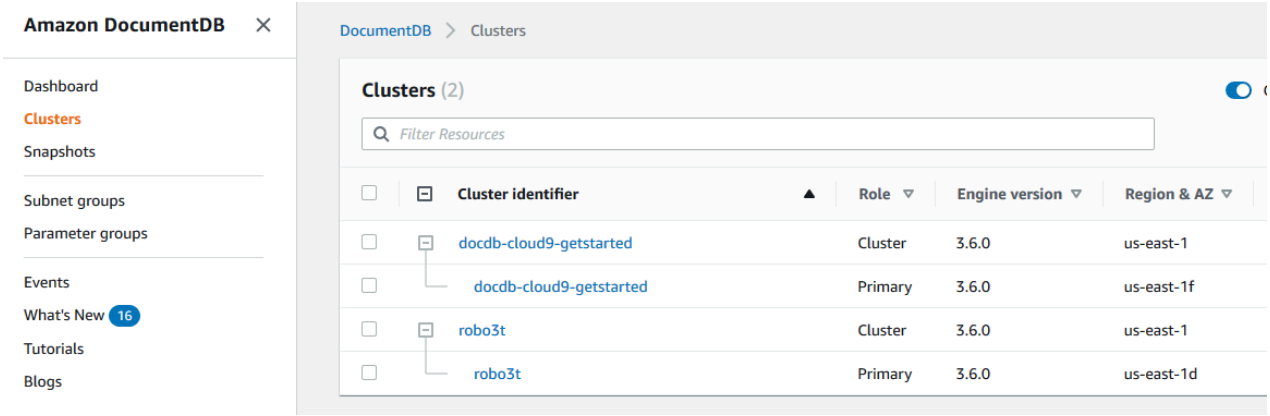
1. Determine el grupo de parámetros de clúster que utiliza el clúster.

   a. Abra la consola de Amazon DocumentDB en https://console.aws.amazon.com/docdb.

b. En el panel de navegación, seleccione Clusters (Clústeres).

> **Tip**
>
> Si no ve el panel de navegación del lado izquierdo de la pantalla, seleccione el icono de menú
> (≡)
> en la esquina superior izquierda de la página.

c. Tenga en cuenta que en el cuadro de navegación Clústeres, la columna Identificador del clústeres muestra tanto los clústeres como las instancias. Las instancias se muestran debajo de los clústeres. Consulte la siguiente captura de pantalla como referencia.



d. Elija el clúster que le interese.

e. Elija la pestaña de Configuración, desplácese hacia abajo hasta la parte inferior de Detalles del clúster) y localice el Grupo de parámetros de clúster. Anote el nombre del grupo de parámetros de clúster.

Si el nombre del grupo de parámetros de clúster es `default` (por ejemplo, `default.docdb3.6`), debe crear un grupo de parámetros de clúster personalizado y convertirlo en el grupo de parámetros del clúster antes de continuar. Para obtener más información, consulte los siguientes temas:

1. Creación de grupos de parámetros de clúster de Amazon DocumentDB: si no dispone de un grupo de parámetros de clúster personalizado que pueda utilizar, créelo.
2. Modificación de un clúster de Amazon DocumentDB: modifique el clúster de forma que use el grupo de parámetros de clúster personalizado.

2. Determinar el valor actual del**`tls`** parámetro de clúster.

a. Abra la consola de Amazon DocumentDB en https://console.aws.amazon.com/docdb.

b. En el panel de navegación, seleccione Grupos de parámetros.

c. En la lista de grupos de parámetros de clúster, elija el nombre del grupo de parámetros de clúster que desee.

d. Localice la sección Cluster parameters (Parámetros de clúster). En la lista de parámetros de clúster, localice la `tls` fila del parámetro del clúster. En este punto, las cuatro columnas siguientes son importantes:

- Nombre del parámetro de clúster: el nombre de los parámetros de clúster. Para la administración de TLS, le interesa el `tls` parámetro de clúster.
- Valores: el valor actual de cada parámetro del clúster.
- Valores permitidos: lista de valores que se pueden aplicar a un parámetro de clúster.
- Tipo de aplicación: estática o dinámica. Los cambios en los parámetros de clúster estáticos solo se pueden aplicar al reiniciar las instancias. Los cambios en los parámetros de clúster dinámicos se pueden aplicar inmediatamente o al reiniciar las instancias.

3. Modificar el valor del **`tls`** parámetro de clúster.

Si el valor de `tls` no es el que necesita, modifíquelo para este grupo de parámetros de clúster. Para cambiar el valor del `tls` parámetro de clúster, continúe desde la sección anterior siguiendo los pasos que se indican a continuación.

a. Elija el botón situado a la izquierda del nombre del parámetro de clúster (`tls`).

b. Seleccione Editar.

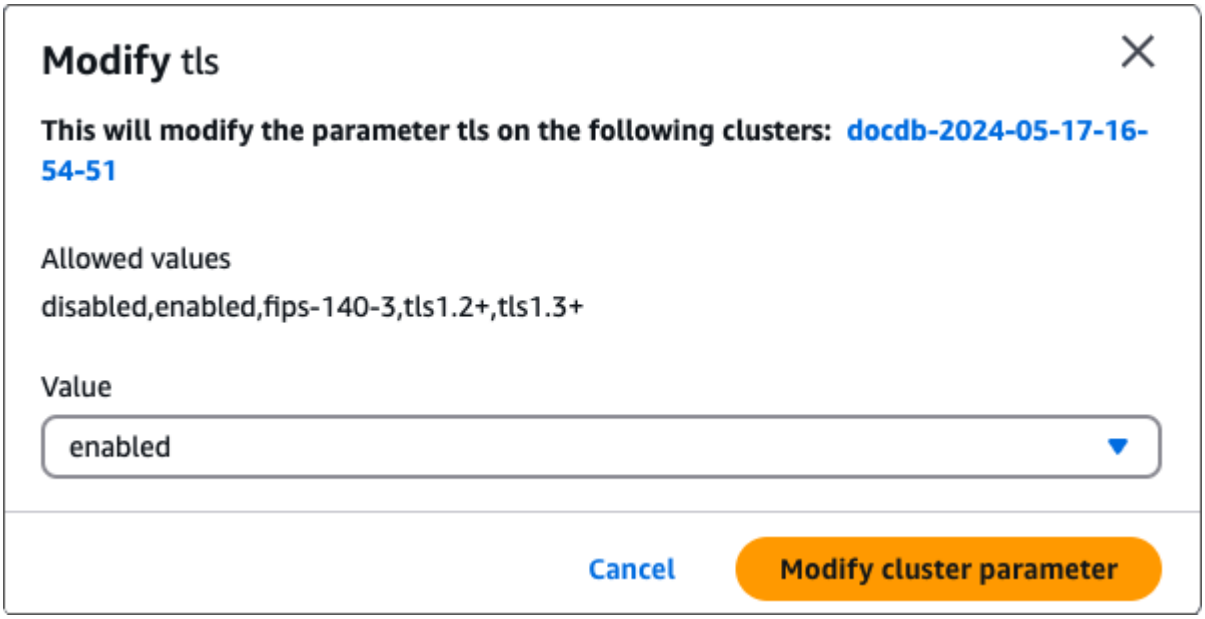
c. Para cambiar el valor de `tls`, en el cuadro de diálogo Modificar**`tls`**, elija el valor que desee para el parámetro de clúster en el menú desplegable.

Los valores válidos son:

- deshabilitado: deshabilita el TLS
- activado: habilita las versiones 1.0 a 1.3 de TLS.
- fips-140-3: habilita TLS con FIPS. El clúster solo acepta conexiones seguras según los requisitos de la publicación 140-3 de las Normas Federales de Proceso de la Información (FIPS). Esto solo se admite a partir de los clústeres de Amazon

DocumentDB 5.0 (versión del motor 3.0.3727) en las siguientes regiones: ca-central-1, us-west-2, us-east-1, us-east-2, us-gov-east-1, us-gov-west-1.

- tls1.2+: habilita las versiones 1.2 y superiores de TLS. Esto solo se admite a partir de Amazon DocumentDB 4.0 (versión de motor 2.0.10980) y Amazon DocumentDB (versión de motor 3.0.11051).
- tls1.3+: habilita las versiones 1.3 y superiores de TLS. Esto solo se admite a partir de Amazon DocumentDB 4.0 (versión de motor 2.0.10980) y Amazon DocumentDB (versión de motor 3.0.11051).



d. Elija Modify cluster parameter (Modificar el parámetro de clúster). El cambio se aplicará a cada instancia del clúster cuando se reinicie.

4. Reinicie la instancia de Amazon DocumentDB.

   Reinicie todas las instancias del clúster para que el cambio se aplique a todas ellas.

   a. Abra la consola de Amazon DocumentDB en https://console.aws.amazon.com/docdb.

   b. En el panel de navegación, seleccione Instances (Instancias).

   c. Para especificar la instancia que se va a reiniciar, búsquela en la lista de instancias y elija el botón situado a la izquierda de su nombre.

   d. Elija Actions (Acciones) y, a continuación, Reboot (Reiniciar). Confirme que desea reiniciar eligiendo Reboot (Reiniciar).

Using the AWS CLI

Siga estos pasos para realizar tareas de administración para el cifrado TLS mediante la AWS CLI, como identificar grupos de parámetros, verificar el valor de TLS y realizar las modificaciones necesarias.

> **Note**
>
> A menos que especifique de manera diferente al crear un clúster, el clúster se crea con el grupo de parámetros de clúster predeterminado. Los parámetros del grupo de parámetros de clúster `default` no se pueden modificar (por ejemplo, `tls` habilitado/deshabilitado). Por lo tanto, si su clúster está utilizando un `default` grupo de parámetros de clúster, debe modificar el clúster para utilizar un grupo de parámetros de clúster no predeterminado. Es posible que primero tenga que crear un grupo de parámetros de clúster personalizado. Para obtener más información, consulte Creación de grupos de parámetros de clúster de Amazon DocumentDB.

1. Determine el grupo de parámetros de clúster que utiliza el clúster.

   Ejecute el comando `describe-db-clusters` con las siguientes opciones:

   - `--db-cluster-identifier`
   - `--query`

   En el siguiente ejemplo, reemplace cada *`marcador de posición del usuario`* con la información de su clúster.

   ```
   aws docdb describe-db-clusters \
     --db-cluster-identifier mydocdbcluster \
     --query 'DBClusters[*].[DBClusterIdentifier,DBClusterParameterGroup]'
   ```

   La salida de esta operación será similar a lo que se indica a continuación (formato JSON):

   ```
   [
       [
           "mydocdbcluster",
           "myparametergroup"
       ]
   ```

```
]
```

Si el nombre del grupo de parámetros de clúster es `default` (es decir, `default.docdb3.6`) debe tener un grupo de parámetros de clúster personalizado y convertirlo en el grupo de parámetros de este clúster antes de continuar. Para obtener más información, consulte los temas siguientes:

1. Creación de grupos de parámetros de clúster de Amazon DocumentDB: si no dispone de un grupo de parámetros de clúster personalizado que pueda utilizar, créelo.
2. Modificación de un clúster de Amazon DocumentDB: modifique el clúster de forma que use el grupo de parámetros de clúster personalizado.

2. Determinar el valor actual del **`tls`** parámetro de clúster.

   Para obtener más información sobre este grupo de parámetros del clúster, ejecute el comando `describe-db-cluster-parameters` con las siguientes opciones:

   - `--db-cluster-parameter-group-name`
   - `--query`

     Limita la salida solo a los campos de interés: `ParameterName`, `ParameterValue`,`AllowedValues` y `ApplyType`.

   En el siguiente ejemplo, reemplace cada *`marcador de posición del usuario`* con la información de su clúster.

```
aws docdb describe-db-cluster-parameters \
  --db-cluster-parameter-group-name myparametergroup \
  --query 'Parameters[*].[ParameterName,ParameterValue,AllowedValues,ApplyType]'
```

   La salida de esta operación será similar a lo que se indica a continuación (formato JSON):

```
[
    [
        "audit_logs",
        "disabled",
        "enabled,disabled",
        "dynamic"
    ],
    [
```

```
        "tls",
        "disabled",
        "disabled,enabled,fips-140-3,tls1.2+,tls1.3+",
        "static"
    ],
    [
        "ttl_monitor",
        "enabled",
        "disabled,enabled",
        "dynamic"
    ]
]
```

3. Modificar el valor del parámetro de clúster**`tls`**.

   Si el valor de `tls` no es el que necesita, modifíquelo para este grupo de parámetros de clúster. Para cambiar el valor del parámetro del clúster `tls`, utilice el comando [`modify-db-cluster-parameter-group`] con las siguientes opciones:

   - `--db-cluster-parameter-group-name`: obligatorio. El nombre del grupo de parámetros de clúster que se va a modificar. No puede ser el grupo de parámetros de clúster`default.*`.
   - `--parameters`: obligatorio. Lista de los parámetros del grupo de parámetros de clúster que se van a modificar.
     - `ParameterName`: obligatorio. El nombre del parámetro de clúster que se va a modificar.
     - `ParameterValue`: obligatorio. El valor nuevo de este parámetro de clúster. Debe ser uno de los del parámetro de clúster `AllowedValues`.
       - `enabled`: el clúster acepta conexiones seguras mediante TLS, versión 1.0 a 1.3.
       - `disabled`: el clúster no acepta conexiones seguras mediante TLS.
       - `fips-140-3`: el clúster solo acepta conexiones seguras según los requisitos de la publicación 140-3 de las Normas Federales de Proceso de la Información (FIPS). Esto solo se admite a partir de los clústeres de Amazon DocumentDB 5.0 (versión del motor 3.0.3727) en las siguientes regiones: ca-central-1, us-west-2, us-east-1, us-east-2, us-gov-east-1, us-gov-west-1.
       - `tls1.2+`: el clúster acepta conexiones seguras mediante TLS, versión 1.2 y superiores. Esto solo se admite a partir de Amazon DocumentDB 4.0 (versión de motor 2.0.10980) y Amazon DocumentDB 5.0 (versión de motor 3.0.11051).

    - `tls1.3+`: el clúster acepta conexiones seguras mediante TLS, versión 1.3 y superiores. Esto solo se admite a partir de Amazon DocumentDB 4.0 (versión de motor 2.0.10980) y Amazon DocumentDB 5.0 (versión de motor 3.0.11051).
- `ApplyMethod`: cuándo se va a aplicar esta modificación. Para los parámetros de clúster estáticos, como `tle`, este valor debe ser `pending-reboot`.
    - `pending-reboot`: el cambio se aplica a una instancia solo después de reiniciarla. Debe reiniciar cada instancia de clúster por separado para que este cambio entre en vigor en todas las instancias del clúster.

En los siguientes ejemplos, reemplace cada *`marcador de posición del usuario`* con la información de su clúster.

El siguiente código deshabilita `tls`, y el cambio se aplica a cada instancia cuando se reinicia.

```
aws docdb modify-db-cluster-parameter-group \
  --db-cluster-parameter-group-name myparametergroup \
  --parameters "ParameterName=tls,ParameterValue=disabled,ApplyMethod=pending-
reboot"
```

El siguiente código habilita `tls` (versión 1.0 a 1.3), y el cambio se aplica a cada instancia cuando se reinicia.

```
aws docdb modify-db-cluster-parameter-group \
  --db-cluster-parameter-group-name myparametergroup \
  --parameters "ParameterName=tls,ParameterValue=enabled,ApplyMethod=pending-
reboot"
```

El siguiente código habilita TLS con `fips-140-3`, y el cambio se aplica a cada instancia cuando se reinicia.

```
aws docdb modify-db-cluster-parameter-group \
  --db-cluster-parameter-group-name myparametergroup2 \
  --parameters "ParameterName=tls,ParameterValue=fips-140-3,ApplyMethod=pending-
reboot"
```

La salida de esta operación será similar a lo que se indica a continuación (formato JSON):

```
{
```

```
    "DBClusterParameterGroupName": "myparametergroup"
}
```

4. Reinicie la instancia de Amazon DocumentDB.

   Reinicie todas las instancias del clúster para que el cambio se aplique a todas ellas. Para reiniciar una instancia de Amazon DocumentDB, utilice el comando `reboot-db-instance` con la siguiente opción:

   - `--db-instance-identifier`

   El siguiente código reinicia la instancia `mydocdbinstance`.

   En los siguientes ejemplos, reemplace cada *marcador de posición del usuario* con la información de su clúster.

   Example

   Para Linux, macOS o Unix:

```
aws docdb reboot-db-instance \
  --db-instance-identifier mydocdbinstance
```

   Para Windows:

```
aws docdb reboot-db-instance ^
  --db-instance-identifier mydocdbinstance
```

   La salida de esta operación será similar a lo que se indica a continuación (formato JSON):

```
{
    "DBInstance": {
        "AutoMinorVersionUpgrade": true,
        "PubliclyAccessible": false,
        "PreferredMaintenanceWindow": "fri:09:32-fri:10:02",
        "PendingModifiedValues": {},
        "DBInstanceStatus": "rebooting",
        "DBSubnetGroup": {
            "Subnets": [
                {
                    "SubnetStatus": "Active",
```

```
                    "SubnetAvailabilityZone": {
                        "Name": "us-east-1a"
                    },
                    "SubnetIdentifier": "subnet-4e26d263"
                },
                {
                    "SubnetStatus": "Active",
                    "SubnetAvailabilityZone": {
                        "Name": "us-east-1c"
                    },
                    "SubnetIdentifier": "subnet-afc329f4"
                },
                {
                    "SubnetStatus": "Active",
                    "SubnetAvailabilityZone": {
                        "Name": "us-east-1e"
                    },
                    "SubnetIdentifier": "subnet-b3806e8f"
                },
                {
                    "SubnetStatus": "Active",
                    "SubnetAvailabilityZone": {
                        "Name": "us-east-1d"
                    },
                    "SubnetIdentifier": "subnet-53ab3636"
                },
                {
                    "SubnetStatus": "Active",
                    "SubnetAvailabilityZone": {
                        "Name": "us-east-1b"
                    },
                    "SubnetIdentifier": "subnet-991cb8d0"
                },
                {
                    "SubnetStatus": "Active",
                    "SubnetAvailabilityZone": {
                        "Name": "us-east-1f"
                    },
                    "SubnetIdentifier": "subnet-29ab1025"
                }
            ],
            "SubnetGroupStatus": "Complete",
            "DBSubnetGroupDescription": "default",
            "VpcId": "vpc-91280df6",
```

```
            "DBSubnetGroupName": "default"
        },
        "PromotionTier": 2,
        "DBInstanceClass": "db.r5.4xlarge",
        "InstanceCreateTime": "2018-11-05T23:10:49.905Z",
        "PreferredBackupWindow": "00:00-00:30",
        "KmsKeyId": "arn:aws:kms:us-east-1:012345678901:key/0961325d-a50b-44d4-
b6a0-a177d5ff730b",
        "StorageEncrypted": true,
        "VpcSecurityGroups": [
            {
                "Status": "active",
                "VpcSecurityGroupId": "sg-77186e0d"
            }
        ],
        "EngineVersion": "3.6.0",
        "DbiResourceId": "db-SAMPLERESOURCEID",
        "DBInstanceIdentifier": "mydocdbinstance",
        "Engine": "docdb",
        "AvailabilityZone": "us-east-1a",
        "DBInstanceArn": "arn:aws:rds:us-east-1:012345678901:db:sample-cluster-
instance-00",
        "BackupRetentionPeriod": 1,
        "Endpoint": {
            "Address": "mydocdbinstance.corcjozrlsfc.us-
east-1.docdb.amazonaws.com",
            "Port": 27017,
            "HostedZoneId": "Z2R2ITUGPM61AM"
        },
        "DBClusterIdentifier": "mydocdbcluster"
    }
}
```

El reinicio de la instancia puede tardar unos minutos. Solo puede usar la instancia cuando su estado sea available (disponible). Puede monitorizar el estado de la instancia mediante la consola o la AWS CLI. Para obtener más información, consulte Supervisión del estado de un clúster de Amazon DocumentDB.

Administración de claves

Amazon DocumentDB usa AWS Key Management Service (AWS KMS) para recuperar y administrar las claves de cifrado. AWS KMS combina hardware y software seguros y altamente disponibles para ofrecer un sistema de administración de claves escalado para la nube. Si utiliza AWS KMS, puede crear claves de cifrado y definir las políticas que controlan cómo se pueden utilizar dichas claves. AWS KMS es compatible con AWS CloudTrail, lo que permite auditar el uso de claves para comprobar que las claves se utilizan de forma adecuada.

Puede usar sus claves AWS KMS junto con Amazon DocumentDB y servicios de AWS compatibles como Amazon Simple Storage Service (Amazon S3), Amazon Relational Database Service (Amazon RDS), Amazon Elastic Block Store (Amazon EBS) y Amazon Redshift. Para obtener una lista de los servicios que admiten AWS KMS, consulte Cómo los servicios de AWS usan AWS KMS en la Guía para desarrolladores de AWS Key Management Service. Para obtener más información sobre AWS KMS, consulte ¿Qué es AWS Key Management Service?

Identity and Access Management para Amazon DocumentDB

AWS Identity and Access Management (IAM) es una herramienta Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a los AWS recursos. Los administradores de IAM controlan quién se puede autenticar (iniciar sesión) y autorizar (tener permisos) para utilizar los recursos de Amazon DocumentDB. La IAM es una Servicio de AWS herramienta que puede utilizar sin coste adicional.

Temas

- Público
- Autenticación con identidades
- Administración del acceso con políticas
- Cómo funciona Amazon DocumentDB con IAM
- Ejemplos de políticas basadas en identidades para Amazon DocumentDB
- Solución de problemas de identidad y acceso de Amazon DocumentDB
- Administración de permisos de acceso para los recursos de Amazon DocumentDB
- Uso de políticas basadas en identidad (políticas de IAM) para Amazon DocumentDB

- AWS políticas administradas para Amazon DocumentDB
- Permisos de la API de Amazon DocumentDB: referencia de acciones, recursos y condiciones

Público

La forma de usar AWS Identity and Access Management (IAM) varía según la función que desempeñes:

- Usuario del servicio: solicita permisos a su administrador si no puede acceder a las características (consulte Solución de problemas de identidad y acceso de Amazon DocumentDB).
- Administrador del servicio: determina el acceso de los usuarios y envía solicitudes de permiso (consulte Cómo funciona Amazon DocumentDB con IAM).
- Administrador de IAM: escribe políticas para administrar el acceso (consulte Ejemplos de políticas basadas en identidades para Amazon DocumentDB).

Autenticación con identidades

La autenticación es la forma en que inicias sesión AWS con tus credenciales de identidad. Debe autenticarse como usuario de Usuario raíz de la cuenta de AWS IAM o asumir una función de IAM.

Puede iniciar sesión como una identidad federada con las credenciales de una fuente de identidad, como AWS IAM Identity Center (IAM Identity Center), la autenticación de inicio de sesión único o las credenciales. Google/Facebook Para obtener más información sobre el inicio de sesión, consulte Cómo iniciar sesión en su Cuenta de AWS en la Guía del usuario de AWS Sign-In .

Para el acceso programático, AWS proporciona un SDK y una CLI para firmar criptográficamente las solicitudes. Para obtener más información, consulte AWS Signature Version 4 para solicitudes de API en la Guía del usuario de IAM.

Cuenta de AWS usuario root

Al crear un Cuenta de AWS, se comienza con una identidad de inicio de sesión denominada usuario Cuenta de AWS raíz que tiene acceso completo a todos Servicios de AWS los recursos. Recomendamos encarecidamente que no utilice el usuario raíz para sus tareas diarias. Para ver las tareas que requieren credenciales de usuario raíz, consulte Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos que utilicen la federación con un proveedor de identidades para acceder Servicios de AWS mediante credenciales temporales.

Una identidad federada es un usuario del directorio empresarial, del proveedor de identidades web o al Directory Service que se accede Servicios de AWS mediante credenciales de una fuente de identidad. Las identidades federadas asumen roles que proporcionan credenciales temporales.

Para una administración de acceso centralizada, recomendamos AWS IAM Identity Center. Para obtener más información, consulte ¿Qué es el Centro de identidades de IAM? en la Guía del usuario de AWS IAM Identity Center .

Usuarios y grupos de IAM

Un usuario de IAM es una identidad que dispone de permisos específicos para una sola persona o aplicación. Recomendamos usar credenciales temporales en lugar de usuarios de IAM con credenciales a largo plazo. Para obtener más información, consulte Exigir a los usuarios humanos que utilicen la federación con un proveedor de identidad para acceder AWS mediante credenciales temporales en la Guía del usuario de IAM.

Un grupo de IAM especifica una colección de usuarios de IAM y facilita la administración de permisos para grandes conjuntos de usuarios. Para obtener más información, consulte Casos de usos para usuarios de IAM en la Guía del usuario de IAM.

Roles de IAM

Un rol de IAM es una identidad con permisos específicos que proporciona credenciales temporales. Puede asumir un rol cambiando de un rol de usuario a uno de IAM (consola) o llamando a una AWS CLI operación de AWS API. Para obtener más información, consulte Métodos para asumir un rol en la Guía del usuario de IAM.

Las funciones de IAM son útiles para el acceso de usuarios federados, los permisos de usuario de IAM temporales, el acceso entre cuentas, el acceso entre servicios y las aplicaciones que se ejecutan en Amazon. EC2 Para obtener más información, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Administración del acceso con políticas

El acceso se controla creando políticas y AWS adjuntándolas a identidades o recursos. AWS Una política define los permisos cuando están asociados a una identidad o un recurso. AWS evalúa estas

políticas cuando un director hace una solicitud. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre los documentos de política JSON, consulte Información general de políticas de JSON en la Guía del usuario de IAM.

Mediante las políticas, los administradores especifican quién tiene acceso a qué, definiendo qué entidad principal puede realizar acciones sobre qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Un administrador de IAM crea políticas de IAM y las agrega a roles, que los usuarios pueden asumir posteriormente. Las políticas de IAM definen permisos independientemente del método que se utilice para realizar la operación.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de política de permisos JSON que asocia a una identidad (usuario, grupo o rol). Estas políticas controlan qué acciones pueden realizar las identidades, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en la identidad, consulte Definición de permisos de IAM personalizados con políticas administradas por el cliente en la Guía del usuario de IAM.

Las políticas basadas en identidad pueden ser políticas insertadas (incrustadas directamente en una sola identidad) o políticas administradas (políticas independientes asociadas a varias identidades). Para obtener más información sobre cómo elegir una política administrada o una política insertada, consulte Elegir entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de políticas JSON que se asocian a un recurso. Los ejemplos incluyen políticas de confianza de roles de IAM y políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Debe especificar una entidad principal en una política basada en recursos.

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No puedes usar políticas AWS gestionadas de IAM en una política basada en recursos.

Otros tipos de políticas

AWS admite tipos de políticas adicionales que pueden establecer los permisos máximos que conceden los tipos de políticas más comunes:

- Límites de permisos: establecen los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM. Para obtener más información, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.
- Políticas de control de servicios (SCPs): especifican los permisos máximos para una organización o unidad organizativa en AWS Organizations. Para obtener más información, consulte Políticas de control de servicios en la Guía del usuario de AWS Organizations .
- Políticas de control de recursos (RCPs): establece los permisos máximos disponibles para los recursos de tus cuentas. Para obtener más información, consulte Políticas de control de recursos (RCPs) en la Guía del AWS Organizations usuario.
- Políticas de sesión: políticas avanzadas que se transfieren como parámetro cuando se crea una sesión temporal para un rol o un usuario federado. Para obtener más información, consulte Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo se AWS determina si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la lógica de evaluación de políticas en la Guía del usuario de IAM.

Cómo funciona Amazon DocumentDB con IAM

Antes de utilizar IAM para administrar el acceso a Amazon DocumentDB, obtenga información sobre qué características de IAM se encuentran disponibles con Amazon DocumentDB.

Características de IAM que puede utilizar con Amazon DocumentDB

Característica de IAM	Clústeres basados en instancias	Clústeres elásticos
Políticas basadas en identidades	Sí	Sí
Políticas basadas en recursos	No	No
Acciones de políticas	Sí	Sí

Característica de IAM	Clústeres basados en instancias	Clústeres elásticos
Recursos de políticas	Sí	Sí
Claves de condición de política (específicas del servicio)	Sí	Sí
ACLs	No	No
ABAC (etiquetas en políticas)	Parcial	Sí
Credenciales temporales	Sí	Sí
Permisos de entidades principales	Sí	Sí
Roles de servicio	Sí	Sí
Roles vinculados al servicio	No	Sí

Para obtener una visión general de cómo funcionan Amazon DocumentDB y otros AWS servicios con la mayoría de las características de IAM, consulte los AWS servicios que funcionan con IAM en la Guía del usuario de IAM.

Políticas de Amazon DocumentDB basadas en identidades

Compatibilidad con las políticas basadas en identidad: sí

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en la identidad, consulte Definición de permisos de IAM personalizados con políticas administradas por el cliente en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones.

Para obtener más información sobre los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de la política de JSON de IAM en la Guía del usuario de IAM.

Ejemplos de políticas basadas en identidades para Amazon DocumentDB

Para ver ejemplos de políticas basadas en identidad de Amazon DocumentDB, consulte Ejemplos de políticas basadas en identidades para Amazon DocumentDB.

Políticas basadas en recursos de Amazon DocumentDB

Admite políticas basadas en recursos: no

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Los ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política basada en recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Para obtener más información, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Acciones de políticas para Amazon DocumentDB

Compatibilidad con las acciones de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

> **Note**
>
> Para determinadas funciones de administración, Amazon DocumentDB utiliza tecnología operativa que se comparte con Amazon Relational Database Service (Amazon RDS).

Para ver una lista de las acciones de Amazon DocumentDB, consulte Acciones definidas por el servicio de base de datos relacional de Amazon en la Referencia de autorizaciones de servicio.
Para ver las acciones de políticas para los clústeres elásticos de Amazon DocumentDB, consulte Acciones definidas por los clústeres elásticos de Amazon DocumentDB en la Referencia de autorización de servicios.

Las acciones de políticas de Amazon DocumentDB utilizan el siguiente prefijo antes de la acción:

```
aws
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

```
"Action": [
      "aws:action1",
      "aws:action2"
         ]
```

Para ver ejemplos de políticas basadas en identidad de Amazon DocumentDB, consulte Ejemplos de políticas basadas en identidades para Amazon DocumentDB.

Recursos de políticas para Amazon DocumentDB

Compatibilidad con los recursos de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). En el caso de las acciones que no admiten permisos por recurso, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

```
"Resource": "*"
```

> **Note**
>
> Para determinadas funciones de administración, Amazon DocumentDB utiliza tecnología operativa que se comparte con Amazon Relational Database Service (Amazon RDS). Para ver una lista de los tipos de recursos de RDS y sus tipos ARNs, consulte Recursos definidos por Amazon Relational Database Service en la Referencia de autorización de servicios. Para obtener información acerca de las acciones con las que puede especificar el ARN de cada recurso, consulte Acciones definidas por el servicio de base de datos relacional de Amazon.
>
> Para ver los tipos de recursos para los clústeres elásticos de Amazon DocumentDB, consulte Tipos de recursos definidos por los clústeres elásticos de Amazon DocumentDB en la Referencia de autorización de servicios.

Para ver ejemplos de políticas basadas en identidad de Amazon DocumentDB, consulte Ejemplos de políticas basadas en identidades para Amazon DocumentDB.

Claves de condición de políticas para Amazon DocumentDB

Compatibilidad con claves de condición de políticas específicas del servicio: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` especifica cuándo se ejecutan las instrucciones en función de criterios definidos. Puede crear expresiones condicionales que utilizan operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

> **Note**
>
> Para determinadas funciones de administración, Amazon DocumentDB utiliza tecnología operativa que se comparte con Amazon Relational Database Service (Amazon RDS). Para obtener una lista de las claves de condición de Amazon ECS, consulte Claves de condición del servicio de base de datos relacional de Amazon en la Referencia de autorizaciones de servicio. Para obtener más información acerca de las acciones y los

recursos con los que puede utilizar una clave de condición, consulte Acciones definidas por el servicio de base de datos relacional de Amazon.
Para ver las claves de condición para los clústeres elásticos de Amazon DocumentDB, consulte Claves de condición de los clústeres elásticos de Amazon DocumentDB en la Referencia de autorización de servicios.

Para ver ejemplos de políticas basadas en identidad de Amazon DocumentDB, consulte Ejemplos de políticas basadas en identidades para Amazon DocumentDB.

ACLs en Amazon DocumentDB

Soporta ACLs: No

Las listas de control de acceso (ACLs) controlan qué directores (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLs son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

ABAC con Amazon DocumentDB

> **Note**
>
> ABAC solo es compatible parcialmente con los clústeres basados en instancias, pero es compatible con los clústeres elásticos.

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos denominados etiquetas. Puede adjuntar etiquetas a las entidades y AWS los recursos de IAM y, a continuación, diseñar políticas de ABAC para permitir las operaciones cuando la etiqueta del director coincida con la etiqueta del recurso.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte Definición de permisos con la autorización de ABAC en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulte Uso del control de acceso basado en atributos (ABAC) en la Guía del usuario de IAM.

Uso de credenciales temporales con Amazon DocumentDB

Compatibilidad con credenciales temporales: sí

Las credenciales temporales proporcionan acceso a AWS los recursos a corto plazo y se crean automáticamente cuando se utiliza la federación o se cambia de rol. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para obtener más información, consulte Credenciales de seguridad temporales en IAM y Servicios de AWS que funcionan con IAM en la Guía del usuario de IAM.

Permisos de entidades principales entre servicios de Amazon DocumentDB

Admite sesiones de acceso directo (FAS): sí

Las sesiones de acceso directo (FAS) utilizan los permisos del principal que llama y los que solicitan Servicio de AWS para realizar solicitudes a los servicios descendentes. Servicio de AWS Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Sesiones de acceso directo.

Roles de servicio para Amazon DocumentDB

Compatible con roles de servicio: sí

Un rol de servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Crear un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

> **Warning**
>
> Cambiar los permisos de un rol de servicio podría interrumpir la funcionalidad de Amazon DocumentDB. Edite los roles de servicio solo cuando Amazon DocumentDB proporcione orientación para hacerlo.

Roles vinculados a servicios para Amazon DocumentDB

> **Note**
>
> Los roles vinculados a servicios no son compatibles con los clústeres basados en instancias, pero sí con los clústeres elásticos.

Un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Para más información sobre cómo crear o administrar roles vinculados a servicios, consulta Servicios de AWS que funcionan con IAM. Busque un servicio en la tabla que incluya `Yes` en la columna Rol vinculado a un servicio. Seleccione el vínculo Sí para ver la documentación acerca del rol vinculado a servicios para ese servicio.

Ejemplos de políticas basadas en identidades para Amazon DocumentDB

De forma predeterminada, los usuarios y roles no tienen permiso para crear ni modificar los recursos de Amazon DocumentDB. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte Creación de políticas de IAM (consola) en la Guía del usuario de IAM.

Para obtener más información sobre las acciones y los tipos de recursos definidos por Amazon DocumentDB, incluido el formato de cada uno de los tipos de recursos, consulte Acciones, recursos y claves de condición de Amazon Relational Database Service en la Referencia de autorización de servicios. ARNs

> **Note**
>
> Para determinadas funciones de administración, Amazon DocumentDB utiliza tecnología operativa que se comparte con Amazon Relational Database Service (Amazon RDS).

Para conocer las acciones de políticas para los clústeres elásticos de Amazon DocumentDB, consulte Acciones, recursos y claves de condición de los clústeres elásticos de Amazon DocumentDB en la Referencia de autorización de servicios.

Temas

- Prácticas recomendadas sobre las políticas
- Uso de la consola de Amazon DocumentDB
- Cómo permitir a los usuarios consultar sus propios permisos

Prácticas recomendadas sobre las políticas

Las políticas basadas en identidades determinan si alguien puede crear, eliminar o acceder a los recursos de Amazon DocumentDB de la cuenta. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulte las políticas administradas por AWS o las políticas administradas por AWS para funciones de tarea en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte Políticas y permisos en IAM en la Guía del usuario de IAM.
- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo CloudFormation. Para obtener más información, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.

- Utiliza el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte Validación de políticas con el Analizador de acceso de IAM en la Guía del usuario de IAM.
- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para exigir la MFA cuando se invoquen las operaciones de la API, añada condiciones de MFA a sus políticas. Para más información, consulte Acceso seguro a la API con MFA en la Guía del usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

Uso de la consola de Amazon DocumentDB

Para acceder a la consola de Amazon DocumentDB (con compatibilidad con MongoDB) , debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver detalles sobre los recursos de Amazon DocumentDB en su. Cuenta de AWS Si crea una política basada en identidades que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles) que tengan esa política.

No necesita conceder permisos mínimos de consola a los usuarios que solo realizan llamadas a la API AWS CLI o a la AWS API. En su lugar, permita el acceso únicamente a las acciones que coincidan con la operación de API que intentan realizar.

Para garantizar que los usuarios y los roles puedan seguir utilizando la consola de Amazon DocumentDB, adjunte también la Amazon `ConsoleAccess` DocumentDB `ReadOnly` AWS o la política gestionada a las entidades. Para obtener más información, consulte Adición de permisos a un usuario en la Guía del usuario de IAM:

Cómo permitir a los usuarios consultar sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas administradas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante la API o. AWS CLI AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Solución de problemas de identidad y acceso de Amazon DocumentDB

Utilice la siguiente información para diagnosticar y solucionar los problemas comunes que es posible que surjan cuando se trabaja con Amazon DocumentDB e IAM.

Temas

- No tengo autorización para realizar una acción en Amazon DocumentDB

- No estoy autorizado a realizar tareas como: PassRole
- Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis recursos de Amazon DocumentDB

No tengo autorización para realizar una acción en Amazon DocumentDB

Si recibe un error que indica que no tiene autorización para realizar una acción, las políticas se deben actualizar para permitirle realizar la acción.

En el siguiente ejemplo, el error se produce cuando el usuario de IAM `mateojackson` intenta utilizar la consola para consultar los detalles acerca de un recurso ficticio *`my-example-widget`*, pero no tiene los permisos ficticios `aws:`*`GetWidget`*.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 aws:GetWidget on resource: my-example-widget
```

En este caso, la política del usuario `mateojackson` debe actualizarse para permitir el acceso al recurso *`my-example-widget`* mediante la acción `aws:`*`GetWidget`*.

Si necesitas ayuda, ponte en contacto con tu administrador. AWS El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

No estoy autorizado a realizar tareas como: PassRole

Si recibe un error que indica que no tiene autorización para llevar a cabo la acción `iam:PassRole`, las políticas se deben actualizar para permitirle pasar un rol a Amazon DocumentDB.

Algunas Servicios de AWS permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada a un servicio. Para ello, debe tener permisos para transferir la función al servicio.

En el siguiente ejemplo, el error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en Amazon DocumentDB. Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su AWS administrador. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis recursos de Amazon DocumentDB

Se puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Se puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admiten políticas basadas en recursos o listas de control de acceso (ACLs), puede usar esas políticas para permitir que las personas accedan a sus recursos.

Para obtener más información, consulte lo siguiente:

- Para saber si Amazon DocumentDB admite estas características, consulte Cómo funciona Amazon DocumentDB con IAM.
- Para obtener información sobre cómo proporcionar acceso a los recursos de su Cuentas de AWS propiedad, consulte Proporcionar acceso a un usuario de IAM en otro de su propiedad en la Cuenta de AWS Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo proporcionar acceso a recursos que Cuentas de AWS son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulte Proporcionar acceso a usuarios autenticados externamente (federación de identidades) en la Guía del usuario de IAM.
- Para conocer sobre la diferencia entre las políticas basadas en roles y en recursos para el acceso entre cuentas, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Administración de permisos de acceso para los recursos de Amazon DocumentDB

Cada AWS recurso es propiedad de una persona Cuenta de AWS, y los permisos para crearlos o acceder a ellos se rigen por las políticas de permisos. Un administrador de cuentas puede adjuntar

políticas de permisos a las identidades de IAM (es decir, usuarios, grupos y roles), y algunos servicios (por ejemplo AWS Lambda) también permiten adjuntar políticas de permisos a los recursos.

> **Note**
>
> Un administrador de la cuenta (o usuario administrador) es un usuario con permisos de administrador. Para obtener más información, consulte Prácticas recomendadas de IAM en la Guía del usuario de IAM.

Temas

- Recursos y operaciones de Amazon DocumentDB
- Titularidad de los recursos
- Administración del acceso a los recursos
- Especificación de elementos de política: acciones, efectos, recursos y entidades principales
- Especificación de las condiciones de una política

Recursos y operaciones de Amazon DocumentDB

En Amazon DocumentDB, el recurso principal es un clúster. Amazon DocumentDB admite otros recursos que pueden utilizarse con el recurso principal, como las instancias, los grupos de parámetros y las suscripciones a eventos. Estos recursos se denominan subrecursos.

Estos recursos y subrecursos tienen nombres de recursos de Amazon (ARNs) exclusivos asociados a ellos, como se muestra en la siguiente tabla.

Tipo de recurso	Formato de ARN
Clúster	`arn:aws:rds:` *`region`*`:`*`account-id`* `:cluster:` *`db-cluster-name`*
Grupo de parámetros del clúster	`arn:aws:rds:` *`region`*`:`*`account-id`* `:cluster-pg:` *`cluster-parameter-group-name`*
Instantánea de clúster	`arn:aws:rds:` *`region`*`:`*`account-id`* `:cluster-snapshot:` *`cluster-snapshot-name`*

Tipo de recurso	Formato de ARN
Instancia	`arn:aws:rds:` *`region`*`:`*`account-id`* `:db:`*`db-instance-name`*
Security group (Grupo de seguridad)	`arn:aws:rds:` *`region`*`:`*`account-id`* `:secgrp:`*`security-group-name`*
Grupo de subredes	`arn:aws:rds:` *`region`*`:`*`account-id`* `:subgrp:`*`subnet-group-name`*

Amazon DocumentDB proporciona un conjunto de operaciones para trabajar con los recursos de Amazon DocumentDB. Para obtener una lista de operaciones disponibles, consulte Acciones.

Titularidad de los recursos

El propietario de un recurso es Cuenta de AWS quien creó un recurso. Es decir, el propietario del recurso es la Cuenta de AWS entidad principal (la cuenta raíz, un usuario de IAM o un rol de IAM) que autentica la solicitud que crea el recurso. Los siguientes ejemplos ilustran cómo funciona:

- Si utiliza las credenciales de su cuenta raíz Cuenta de AWS para crear un recurso de Amazon DocumentDB, como una instancia, Cuenta de AWS es el propietario del recurso de Amazon DocumentDB.
- Si crea un usuario de IAM en su cuenta Cuenta de AWS y concede permisos para crear recursos de Amazon DocumentDB a ese usuario, el usuario podrá crear recursos de Amazon DocumentDB. Sin embargo, usted Cuenta de AWS, al que pertenece el usuario, es propietario de los recursos de Amazon DocumentDB.
- Si crea una función de IAM Cuenta de AWS con permisos para crear recursos de Amazon DocumentDB, cualquier persona que pueda asumir la función podrá crear recursos de Amazon DocumentDB. La suya Cuenta de AWS, a la que pertenece la función, es propietaria de los recursos de Amazon DocumentDB.

Administración del acceso a los recursos

Una política de permisos describe quién tiene acceso a qué. En la siguiente sección se explican las opciones disponibles para crear políticas de permisos.

> **Note**
>
> En esta sección, también se explica el uso de IAM en el contexto de Amazon DocumentDB. No se proporciona información detallada sobre el servicio de IAM. Para ver la documentación completa de IAM, consulte ¿Qué es IAM? en la Guía del usuario de IAM. Para obtener más información acerca de la sintaxis y las descripciones de la política de IAM, consulte Referencia de políticas de IAM de AWS en la Guía del usuario de IAM.

Las políticas que se asocian a una identidad de IAM se denominan políticas basadas en la identidad (políticas de IAM). Las políticas que se asocian a un recurso se denominan "políticas basadas en recursos". Amazon DocumentDB solo admite políticas basadas en identidad (políticas del IAM).

Temas

- Políticas basadas en identidades (políticas de IAM)
- Políticas basadas en recursos

Políticas basadas en identidades (políticas de IAM)

Puede asociar políticas a identidades de IAM. Por ejemplo, puede hacer lo siguiente:

- Asociar una política de permisos a un usuario o un grupo de su cuenta: un administrador de la cuenta puede utilizar una política de permisos asociada a un usuario determinado para concederle permisos para crear un recurso de Amazon DocumentDB, como una instancia.
- Adjuntar una política de permisos a un rol (conceder permisos para cuentas cruzadas): puede adjuntar una política de permisos basada en identidades a un rol de IAM para conceder permisos para cuentas cruzadas. Por ejemplo, un administrador puede crear un rol para conceder permisos entre cuentas a otro Cuenta de AWS o a un AWS servicio de la siguiente manera:
  1. El administrador de la CuentaA crea un rol de IAM y asocia una política de permisos a dicho rol, que concede permisos sobre los recursos de la CuentaA.
  2. El administrador de la CuentaA asocia una política de confianza al rol que identifica la Cuenta B como la entidad principal que puede asumir el rol.
  3. De este modo, el administrador de la cuenta B puede delegar los permisos para que asuman la función en cualquier usuario de la cuenta B. De este modo, los usuarios de la cuenta B pueden crear recursos de la cuenta A. El responsable de la política de confianza también puede ser el

director de AWS servicio si desea conceder permisos a un AWS servicio para que asuma esa función.

Para obtener más información sobre el uso de IAM para delegar permisos, consulte Administración de accesos en la Guía del usuario de IAM.

A continuación se muestra un ejemplo de una política que permite al usuario con el ID `123456789012` crear instancias para una Cuenta de AWS. La nueva instancia debe usar un grupo de opciones y un grupo de parámetros de base de datos que comience por `default` y debe utilizar el grupo de subredes `default`.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCreateDBInstanceOnly",
            "Effect": "Allow",
            "Action": [
                "rds:CreateDBInstance"
            ],
            "Resource": [
                "arn:aws:rds:*:123456789012:db:test*",
                "arn:aws:rds:*:123456789012:pg:cluster-pg:default*",
                "arn:aws:rds:*:123456789012:subgrp:default"
            ]
        }
    ]
}
```

Para obtener más información acerca del uso de políticas basadas en identidades con Amazon DocumentDB, consulte Uso de políticas basadas en identidad (políticas de IAM) para Amazon DocumentDB. Para obtener más información sobre usuarios, grupos, roles y permisos, consulte Identidades (usuarios, grupos y roles) en la Guía del usuario de IAM.

Políticas basadas en recursos

Otros servicios de, como Amazon Simple Storage Service (Amazon S3), también admiten políticas de permisos basadas en recursos. Por ejemplo, puede adjuntar una política a un bucket de Amazon S3 para administrar los permisos de acceso a dicho bucket. Amazon DocumentDB no admite políticas basadas en recursos.

Especificación de elementos de política: acciones, efectos, recursos y entidades principales

Para cada recurso de Amazon DocumentDB (consulte Recursos y operaciones de Amazon DocumentDB), el servicio define un conjunto de operaciones de API. Para obtener más información, consulte Acciones. Para conceder permisos para estas operaciones de la API, Amazon DocumentDB define un conjunto de acciones que usted puede especificar en una política. Para realizar una operación API pueden ser necesarios permisos para más de una acción.

A continuación, se indican los elementos básicos de la política:

- Recurso: en una política, se usa un nombre de recurso de Amazon (ARN) para identificar el recurso al que se aplica la política.
- Acción: utilice palabras clave de acción para identificar las operaciones del recurso que desea permitir o denegar. Por ejemplo, cuando se concede el permiso `rds:DescribeDBInstances`, el usuario puede realizar la operación `DescribeDBInstances`.
- Efecto: especifique el efecto que se producirá cuando el usuario solicite la acción específica; puede ser permitir o denegar. Si no concede acceso de forma explícita (permitir) a un recurso, el acceso se deniega implícitamente. También puede denegar explícitamente el acceso a un recurso para asegurarse de que un usuario no pueda obtener acceso a él, aunque otra política le conceda acceso.
- Entidad principal: en las políticas basadas en identidades (políticas de IAM), el usuario al que se asocia esta política es la entidad principal implícita. Para las políticas basadas en recursos, debe especificar el usuario, la cuenta, el servicio u otra entidad que desee que reciba permisos (se aplica solo a las políticas basadas en recursos). Amazon DocumentDB no admite políticas basadas en recursos.

Para obtener más información sobre la sintaxis y descripciones de las políticas de IAM, consulte Referencia de la política de IAM de AWS en la Guía del usuario de IAM.

Para ver una tabla con todas las acciones de la API de Amazon DocumentDB y los recursos a los que se aplican, consulte Permisos de la API de Amazon DocumentDB: referencia de acciones, recursos y condiciones.

Especificación de las condiciones de una política

Al conceder permisos, puede utilizar el lenguaje de la política de IAM para especificar las condiciones en la que se debe aplicar una política. Por ejemplo, es posible que desee que solo se aplique una política después de una fecha específica. Para obtener más información sobre cómo especificar condiciones en un lenguaje de política, consulte Condition en la Guía del usuario de IAM.

Para expresar condiciones, se usan claves de condición predefinidas. Amazon DocumentDB no tiene claves de contexto específicas de servicios que se puedan utilizar en una política de IAM. Para obtener una lista de las claves de contexto de condición que están disponibles para todos los servicios, consulte las claves disponibles para las condiciones en la Guía del usuario de IAM.

Uso de políticas basadas en identidad (políticas de IAM) para Amazon DocumentDB

> **Important**
>
> En determinadas características de administración, Amazon DocumentDB utiliza una tecnología operativa que comparte con Amazon RDS. Las llamadas a la consola y a la API de Amazon DocumentDB se registran como llamadas realizadas a la API de Amazon RDS.
>
> AWS CLI
>
> Le recomendamos que consulte primero los temas de introducción en los que se explican los conceptos básicos y las opciones disponibles para administrar el acceso a sus recursos de Amazon DocumentDB. Para obtener más información, consulte Administración de permisos de acceso para los recursos de Amazon DocumentDB.

Este tema contiene ejemplos de políticas basadas en identidades, donde los administradores de cuentas pueden asociar políticas de permisos a identidades de IAM (es decir, a usuarios, grupos y funciones).

A continuación, se muestra un ejemplo de política de IAM:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCreateDBInstanceOnly",
            "Effect": "Allow",
            "Action": [
                "rds:CreateDBInstance"
            ],
            "Resource": [
                "arn:aws:rds:*:123456789012:db:test*",
                "arn:aws:rds:*:123456789012:pg:cluster-pg:default*",
                "arn:aws:rds:*:123456789012:subgrp:default"
            ]
        }
    ]
}
```

En la política se incluye una sola instrucción que especifica los siguientes permisos para el usuario de IAM:

- La política permite al usuario de IAM crear una instancia mediante la DBInstance acción Crear (esto también se aplica a la create-db-instance AWS CLI operación y a la). Consola de administración de AWS
- El elemento `Resource` especifica que el usuario puede realizar acciones en o con recursos. Puede especificar los recursos mediante un nombre de recurso de Amazon (ARN). Este ARN incluye el nombre del servicio al que pertenece el recurso (`rds`), Región de AWS (*indica cualquier región en este ejemplo), el número de cuenta de usuario (123456789012es el ID de usuario en este ejemplo) y el tipo de recurso.

  El elemento `Resource` del ejemplo especifica las siguientes restricciones políticas en los recursos del usuario:

  - El identificador de instancia para la nueva instancia de base de datos debe comenzar por `test` (por ejemplo, `testCustomerData1`, `test-region2-data`).

- El grupo de parámetros de clúster de la nueva instancia debe empezar por `default`.
- El grupo de subredes de la nueva instancia debe ser el grupo de subredes `default`.

La política no especifica el elemento `Principal`, ya que en una política basada en la identidad no se especifica el elemento principal que obtiene el permiso. Al asociar una política a un usuario, el usuario es la entidad principal implícita. Cuando asocia una política de permisos a un rol de IAM, el elemento principal identificado en la política de confianza de rol obtiene los permisos.

Para ver una tabla con todas las operaciones de la API de Amazon DocumentDB y los recursos a los que se aplican, consulte Permisos de la API de Amazon DocumentDB: referencia de acciones, recursos y condiciones.

Permisos necesarios para usar la consola de Amazon DocumentDB

Para que un usuario pueda trabajar con la consola Amazon DocumentDB, debe tener un conjunto mínimo de permisos. Estos permisos permiten al usuario describir sus recursos de Amazon DocumentDB Cuenta de AWS y proporcionar otra información relacionada, incluida la información de EC2 seguridad y de red de Amazon.

Si crea una política de IAM que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para los usuarios con esa política de IAM. Para asegurarse de que esos usuarios puedan seguir usando la consola Amazon DocumentDB, asocie también la política administrada `AmazonDocDBConsoleFullAccess` al usuario, según se explica en AWS políticas administradas para Amazon DocumentDB.

No es necesario que permita permisos mínimos de consola a los usuarios que solo realicen llamadas a la API AWS CLI o a la API de Amazon DocumentDB.

Ejemplos de políticas administradas por el cliente

En esta sección, encontrará ejemplos de políticas de usuario que conceden permisos para diversas acciones de Amazon DocumentDB. Estas políticas funcionan cuando se utilizan las acciones de la API de Amazon DocumentDB AWS SDKs, o las. AWS CLI Cuando se utiliza la consola, debe conceder permisos adicionales específicos a la consola, tal y como se explica en Permisos necesarios para usar la consola de Amazon DocumentDB.

Para determinadas funciones de administración, Amazon DocumentDB utiliza tecnología operativa que se comparte con Amazon Relational Database Service (Amazon RDS) y Amazon Neptune.

> **Note**
>
> Todos los ejemplos utilizan la región EE.UU. Este (Norte de Virginia) (`us-east-1`) y contienen una cuenta ficticia. IDs

Ejemplos

- Ejemplo 1: permitir que un usuario lleve a cabo cualquier acción Describe con cualquier recurso de Amazon DocumentDB
- Ejemplo 2: prevención de la eliminación de una instancia por parte de un usuario
- Ejemplo 3: prevención de la creación de un clúster por parte de un usuario a menos que el cifrado de almacenamiento esté habilitado

Ejemplo 1: permitir que un usuario lleve a cabo cualquier acción Describe con cualquier recurso de Amazon DocumentDB

La siguiente política de permisos concede permisos a un usuario para ejecutar todas las acciones que empiezan por `Describe`. Estas acciones muestran información acerca de un recurso de Amazon DocumentDB, como una instancia. El carácter comodín (*) del elemento `Resource` indica que las acciones están permitidas en todos los recursos de Amazon DocumentDB que son propiedad de la cuenta.

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"AllowRDSDescribe",
         "Effect":"Allow",
         "Action":"rds:Describe*",
         "Resource":"*"
      }
   ]
}
```

Ejemplo 2: prevención de la eliminación de una instancia por parte de un usuario

La siguiente política de permisos concede permisos para impedir que un usuario elimine una instancia específica. Por ejemplo, puede servir para impedir la eliminación de instancias de producción a cualquier usuario que no sea un administrador.

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"DenyDelete1",
         "Effect":"Deny",
         "Action":"rds:DeleteDBInstance",
         "Resource":"arn:aws:rds:us-east-1:123456789012:db:my-db-instance"
      }
   ]
}
```

Ejemplo 3: prevención de la creación de un clúster por parte de un usuario a menos que el cifrado de almacenamiento esté habilitado

La siguiente política de permisos deniega los permisos a un usuario para crear un clúster de Amazon DocumentDB a menos que se habilite el cifrado de almacenamiento.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Sid": "PreventUnencryptedDocumentDB",
         "Effect": "Deny",
         "Action": "RDS:CreateDBCluster",
         "Condition": {
         "Bool": {
         "rds:StorageEncrypted": "false"
      },
         "StringEquals": {
```

```
            "rds:DatabaseEngine": "docdb"
            }
        },
        "Resource": "*"
        }
    ]
}
```

AWS políticas administradas para Amazon DocumentDB

Para añadir permisos a usuarios, grupos y roles, es más fácil usar políticas AWS administradas que escribirlas usted mismo. Se necesita tiempo y experiencia para crear políticas administradas por el cliente de IAM que proporcionen a su equipo solo los permisos necesarios. Para empezar rápidamente, puedes usar nuestras políticas AWS gestionadas. Estas políticas cubren casos de uso comunes y están disponibles en tu AWS cuenta. Para obtener más información sobre las políticas AWS administradas, consulte las políticas AWS administradas en la Guía del usuario de AWS Identity and Access Management.

AWS los servicios mantienen y AWS actualizan las políticas administradas. No puede cambiar los permisos en las políticas AWS gestionadas. En ocasiones, los servicios añaden permisos adicionales a una política AWS gestionada para admitir nuevas funciones. Este tipo de actualización afecta a todas las identidades (usuarios, grupos y roles) donde se asocia la política. Lo más probable es que los servicios actualicen una política AWS administrada cuando se lanza una nueva función o cuando hay nuevas operaciones disponibles. Los servicios no eliminan los permisos de una política AWS administrada, por lo que las actualizaciones de la política no afectarán a los permisos existentes.

Además, AWS admite políticas administradas para funciones laborales que abarcan varios servicios. Por ejemplo, la política `ViewOnlyAccess` AWS gestionada proporciona acceso de solo lectura a muchos AWS servicios y recursos. Cuando un servicio lanza una nueva función, AWS agrega permisos de solo lectura para nuevas operaciones y recursos. Para obtener una lista y descripciones de las políticas de funciones, consulte Políticas administradas de AWS para funciones de trabajo en la Guía del usuario de la gestión de identidades y accesos de AWS .

Las siguientes políticas AWS gestionadas, que puede adjuntar a los usuarios de su cuenta, son específicas de Amazon DocumentDB:

- AmazonDocDBFullAcceso— Otorga acceso completo a todos los recursos de Amazon DocumentDB para la cuenta raíz AWS .

- AmazonDocDBReadOnlyAccess— Otorga acceso de solo lectura a todos los recursos de Amazon DocumentDB para la cuenta raíz. AWS
- AmazonDocDBConsoleFullAccess: otorga acceso completo para administrar Amazon DocumentDB y los recursos de clústeres elásticos de Amazon DocumentDB mediante la Consola de administración de AWS.
- AmazonDocDBElasticReadOnlyAccess— Otorga acceso de solo lectura a todos los recursos del clúster elástico de Amazon DocumentDB para la cuenta raíz. AWS
- AmazonDocDBElasticFullAccess— Otorga acceso completo a todos los recursos del clúster elástico de Amazon DocumentDB para la cuenta raíz AWS .

AmazonDocDBFullAcceso

Esta política otorga permisos administrativos que brindan a una entidad principal acceso completo a todas las acciones de Amazon DocumentDB. Los permisos de esta política se agrupan de la siguiente manera:

- Los permisos de Amazon DocumentDB permiten todas las acciones de Amazon DocumentDB.
- Algunos de los EC2 permisos de Amazon de esta política son necesarios para validar los recursos aprobados en una solicitud de API. Esto es para garantizar que Amazon DocumentDB pueda utilizar correctamente los recursos con un clúster. El resto de los EC2 permisos de Amazon de esta política permiten a Amazon DocumentDB crear AWS los recursos necesarios para que pueda conectarse a sus clústeres.
- Los permisos de Amazon DocumentDB se utilizan durante las llamadas a la API para validar los recursos transferidos en una solicitud. Son necesarios para que Amazon DocumentDB pueda utilizar la clave pasada con el clúster de Amazon DocumentDB.
- Los CloudWatch registros son necesarios para que Amazon DocumentDB pueda garantizar que se pueda acceder a los destinos de entrega de registros y que sean válidos para el uso de registros por parte de los agentes.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
```

```
            "Action": [
                "rds:AddRoleToDBCluster",
                "rds:AddSourceIdentifierToSubscription",
                "rds:AddTagsToResource",
                "rds:ApplyPendingMaintenanceAction",
                "rds:CopyDBClusterParameterGroup",
                "rds:CopyDBClusterSnapshot",
                "rds:CopyDBParameterGroup",
                "rds:CreateDBCluster",
                "rds:CreateDBClusterParameterGroup",
                "rds:CreateDBClusterSnapshot",
                "rds:CreateDBInstance",
                "rds:CreateDBParameterGroup",
                "rds:CreateDBSubnetGroup",
                "rds:CreateEventSubscription",
                "rds:DeleteDBCluster",
                "rds:DeleteDBClusterParameterGroup",
                "rds:DeleteDBClusterSnapshot",
                "rds:DeleteDBInstance",
                "rds:DeleteDBParameterGroup",
                "rds:DeleteDBSubnetGroup",
                "rds:DeleteEventSubscription",
                "rds:DescribeAccountAttributes",
                "rds:DescribeCertificates",
                "rds:DescribeDBClusterParameterGroups",
                "rds:DescribeDBClusterParameters",
                "rds:DescribeDBClusterSnapshotAttributes",
                "rds:DescribeDBClusterSnapshots",
                "rds:DescribeDBClusters",
                "rds:DescribeDBEngineVersions",
                "rds:DescribeDBInstances",
                "rds:DescribeDBLogFiles",
                "rds:DescribeDBParameterGroups",
                "rds:DescribeDBParameters",
                "rds:DescribeDBSecurityGroups",
                "rds:DescribeDBSubnetGroups",
                "rds:DescribeEngineDefaultClusterParameters",
                "rds:DescribeEngineDefaultParameters",
                "rds:DescribeEventCategories",
                "rds:DescribeEventSubscriptions",
                "rds:DescribeEvents",
                "rds:DescribeOptionGroups",
                "rds:DescribeOrderableDBInstanceOptions",
                "rds:DescribePendingMaintenanceActions",
```

```
                "rds:DescribeValidDBInstanceModifications",
                "rds:DownloadDBLogFilePortion",
                "rds:FailoverDBCluster",
                "rds:ListTagsForResource",
                "rds:ModifyDBCluster",
                "rds:ModifyDBClusterParameterGroup",
                "rds:ModifyDBClusterSnapshotAttribute",
                "rds:ModifyDBInstance",
                "rds:ModifyDBParameterGroup",
                "rds:ModifyDBSubnetGroup",
                "rds:ModifyEventSubscription",
                "rds:PromoteReadReplicaDBCluster",
                "rds:RebootDBInstance",
                "rds:RemoveRoleFromDBCluster",
                "rds:RemoveSourceIdentifierFromSubscription",
                "rds:RemoveTagsFromResource",
                "rds:ResetDBClusterParameterGroup",
                "rds:ResetDBParameterGroup",
                "rds:RestoreDBClusterFromSnapshot",
                "rds:RestoreDBClusterToPointInTime"
            ],
            "Effect": "Allow",
            "Resource": [
                "*"
            ]
        },
        {
            "Action": [
                "cloudwatch:GetMetricStatistics",
                "cloudwatch:ListMetrics",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcAttribute",
                "ec2:DescribeVpcs",
                "kms:ListAliases",
                "kms:ListKeyPolicies",
                "kms:ListKeys",
                "kms:ListRetirableGrants",
                "logs:DescribeLogStreams",
                "logs:GetLogEvents",
                "sns:ListSubscriptions",
                "sns:ListTopics",
```

```
                "sns:Publish"
            ],
            "Effect": "Allow",
            "Resource": [
                "*"
            ]
        },
        {
            "Action": "iam:CreateServiceLinkedRole",
            "Effect": "Allow",
            "Resource": "arn:aws:iam::*:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
            "Condition": {
                "StringLike": {
                    "iam:AWS ServiceName": "rds.amazonaws.com"
                }
            }
        }
    ]
}
```

AmazonDocDBReadOnlyAccess

Esta política otorga permisos de solo lectura que permiten a los usuarios ver información en Amazon DocumentDB. Las entidades principales con esta política asociada no pueden realizar actualizaciones ni eliminar los recursos existentes, ni pueden crear nuevos recursos de Amazon DocumentDB. Por ejemplo, las entidades principales con estos permisos pueden ver la lista de configuraciones y clústeres asociados a su cuenta, pero no pueden cambiar la configuración ni los ajustes de ningún clúster. Los permisos de esta política se agrupan de la siguiente manera:

- Los permisos de Amazon DocumentDB le permiten enumerar los recursos de Amazon DocumentDB, describirlos y obtener información sobre ellos.
- Los EC2 permisos de Amazon se utilizan para describir la VPC de Amazon, las subredes y ENIs los grupos de seguridad asociados a un clúster.
- El permiso de Amazon DocumentDB se utiliza para describir la clave asociada al clúster.

JSON

```
{
```

```
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "rds:DescribeAccountAttributes",
                "rds:DescribeCertificates",
                "rds:DescribeDBClusterParameterGroups",
                "rds:DescribeDBClusterParameters",
                "rds:DescribeDBClusterSnapshotAttributes",
                "rds:DescribeDBClusterSnapshots",
                "rds:DescribeDBClusters",
                "rds:DescribeDBEngineVersions",
                "rds:DescribeDBInstances",
                "rds:DescribeDBLogFiles",
                "rds:DescribeDBParameterGroups",
                "rds:DescribeDBParameters",
                "rds:DescribeDBSubnetGroups",
                "rds:DescribeEventCategories",
                "rds:DescribeEventSubscriptions",
                "rds:DescribeEvents",
                "rds:DescribeOrderableDBInstanceOptions",
                "rds:DescribePendingMaintenanceActions",
                "rds:DownloadDBLogFilePortion",
                "rds:ListTagsForResource"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "cloudwatch:GetMetricStatistics",
                "cloudwatch:ListMetrics"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcAttribute",
```

```
                "ec2:DescribeVpcs"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "kms:ListKeys",
                "kms:ListRetirableGrants",
                "kms:ListAliases",
                "kms:ListKeyPolicies"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "logs:DescribeLogStreams",
                "logs:GetLogEvents"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:logs:*:*:log-group:/aws/rds/*:log-stream:*",
                "arn:aws:logs:*:*:log-group:/aws/docdb/*:log-stream:*"
            ]
        }
    ]
}
```

AmazonDocDBConsoleFullAccess

Otorga acceso completo a la administración de los recursos de Amazon DocumentDB mediante lo siguiente Consola de administración de AWS :

- Los permisos de Amazon DocumentDB permiten todas las acciones de Amazon DocumentDB y de clústeres de Amazon DocumentDB.
- Algunos de los EC2 permisos de Amazon de esta política son necesarios para validar los recursos aprobados en una solicitud de API. Esto es para garantizar que Amazon DocumentDB pueda utilizar correctamente los recursos para ofrecer y mantener un clúster. El resto de los EC2 permisos de Amazon de esta política permiten a Amazon DocumentDB crear AWS los recursos necesarios para que pueda conectarse a sus clústeres, por ejemplo. VPCEndpoint

- AWS KMS los permisos se utilizan durante las llamadas a la API AWS KMS para validar los recursos transferidos en una solicitud. Son necesarios para que Amazon DocumentDB pueda utilizar la clave pasada para cifrar y descifrar los datos en reposo con el clúster elástico de Amazon DocumentDB.
- Los CloudWatch registros son necesarios para que Amazon DocumentDB pueda garantizar que se pueda acceder a los destinos de entrega de los registros y que sean válidos para auditar y perfilar el uso de los registros.
- Los permisos de Secrets Manager son necesarios para validar un secreto determinado y usarlo para configurar el usuario administrador de los clústeres elásticos de Amazon DocumentDB.
- Se requieren permisos de Amazon RDS para las acciones de administración de clústeres de Amazon DocumentDB. En determinadas características de administración, Amazon DocumentDB utiliza una tecnología operativa que comparte con Amazon RDS.
- Los permisos de SNS permiten a las entidades principales acceder a las suscripciones y temas de Amazon Simple Notification Service (Amazon SNS), y publicar mensajes de Amazon SNS.
- Se requieren permisos de IAM para crear los roles vinculados al servicio necesarios para la publicación de métricas y registros.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "DocdbSids",
            "Effect": "Allow",
            "Action": [
                "docdb-elastic:CreateCluster",
                "docdb-elastic:UpdateCluster",
                "docdb-elastic:GetCluster",
                "docdb-elastic:DeleteCluster",
                "docdb-elastic:ListClusters",
                "docdb-elastic:CreateClusterSnapshot",
                "docdb-elastic:GetClusterSnapshot",
                "docdb-elastic:DeleteClusterSnapshot",
                "docdb-elastic:ListClusterSnapshots",
                "docdb-elastic:RestoreClusterFromSnapshot",
                "docdb-elastic:TagResource",
                "docdb-elastic:UntagResource",
```

```
                "docdb-elastic:ListTagsForResource",
                "docdb-elastic:CopyClusterSnapshot",
                "docdb-elastic:StartCluster",
                "docdb-elastic:StopCluster",
                "docdb-elastic:GetPendingMaintenanceAction",
                "docdb-elastic:ListPendingMaintenanceActions",
                "docdb-elastic:ApplyPendingMaintenanceAction",
                "rds:AddRoleToDBCluster",
                "rds:AddSourceIdentifierToSubscription",
                "rds:AddTagsToResource",
                "rds:ApplyPendingMaintenanceAction",
                "rds:CopyDBClusterParameterGroup",
                "rds:CopyDBClusterSnapshot",
                "rds:CopyDBParameterGroup",
                "rds:CreateDBCluster",
                "rds:CreateDBClusterParameterGroup",
                "rds:CreateDBClusterSnapshot",
                "rds:CreateDBInstance",
                "rds:CreateDBParameterGroup",
                "rds:CreateDBSubnetGroup",
                "rds:CreateEventSubscription",
                "rds:CreateGlobalCluster",
                "rds:DeleteDBCluster",
                "rds:DeleteDBClusterParameterGroup",
                "rds:DeleteDBClusterSnapshot",
                "rds:DeleteDBInstance",
                "rds:DeleteDBParameterGroup",
                "rds:DeleteDBSubnetGroup",
                "rds:DeleteEventSubscription",
                "rds:DeleteGlobalCluster",
                "rds:DescribeAccountAttributes",
                "rds:DescribeCertificates",
                "rds:DescribeDBClusterParameterGroups",
                "rds:DescribeDBClusterParameters",
                "rds:DescribeDBClusterSnapshotAttributes",
                "rds:DescribeDBClusterSnapshots",
                "rds:DescribeDBClusters",
                "rds:DescribeDBEngineVersions",
                "rds:DescribeDBInstances",
                "rds:DescribeDBLogFiles",
                "rds:DescribeDBParameterGroups",
                "rds:DescribeDBParameters",
                "rds:DescribeDBSecurityGroups",
                "rds:DescribeDBSubnetGroups",
```

```
                "rds:DescribeEngineDefaultClusterParameters",
                "rds:DescribeEngineDefaultParameters",
                "rds:DescribeEventCategories",
                "rds:DescribeEventSubscriptions",
                "rds:DescribeEvents",
                "rds:DescribeGlobalClusters",
                "rds:DescribeOptionGroups",
                "rds:DescribeOrderableDBInstanceOptions",
                "rds:DescribePendingMaintenanceActions",
                "rds:DescribeValidDBInstanceModifications",
                "rds:DownloadDBLogFilePortion",
                "rds:FailoverDBCluster",
                "rds:ListTagsForResource",
                "rds:ModifyDBCluster",
                "rds:ModifyDBClusterParameterGroup",
                "rds:ModifyDBClusterSnapshotAttribute",
                "rds:ModifyDBInstance",
                "rds:ModifyDBParameterGroup",
                "rds:ModifyDBSubnetGroup",
                "rds:ModifyEventSubscription",
                "rds:ModifyGlobalCluster",
                "rds:PromoteReadReplicaDBCluster",
                "rds:RebootDBInstance",
                "rds:RemoveFromGlobalCluster",
                "rds:RemoveRoleFromDBCluster",
                "rds:RemoveSourceIdentifierFromSubscription",
                "rds:RemoveTagsFromResource",
                "rds:ResetDBClusterParameterGroup",
                "rds:ResetDBParameterGroup",
                "rds:RestoreDBClusterFromSnapshot",
                "rds:RestoreDBClusterToPointInTime"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "DependencySids",
            "Effect": "Allow",
            "Action": [
                "iam:GetRole",
                "cloudwatch:GetMetricData",
                "cloudwatch:GetMetricStatistics",
                "cloudwatch:ListMetrics",
```

```
                "ec2:AllocateAddress",
                "ec2:AssignIpv6Addresses",
                "ec2:AssignPrivateIpAddresses",
                "ec2:AssociateAddress",
                "ec2:AssociateRouteTable",
                "ec2:AssociateSubnetCidrBlock",
                "ec2:AssociateVpcCidrBlock",
                "ec2:AttachInternetGateway",
                "ec2:AttachNetworkInterface",
                "ec2:CreateCustomerGateway",
                "ec2:CreateDefaultSubnet",
                "ec2:CreateDefaultVpc",
                "ec2:CreateInternetGateway",
                "ec2:CreateNatGateway",
                "ec2:CreateNetworkInterface",
                "ec2:CreateRoute",
                "ec2:CreateRouteTable",
                "ec2:CreateSecurityGroup",
                "ec2:CreateSubnet",
                "ec2:CreateVpc",
                "ec2:CreateVpcEndpoint",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAddresses",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeCustomerGateways",
                "ec2:DescribeInstances",
                "ec2:DescribeNatGateways",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribePrefixLists",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroupReferences",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcAttribute",
                "ec2:DescribeVpcEndpoints",
                "ec2:DescribeVpcs",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:ModifySubnetAttribute",
                "ec2:ModifyVpcAttribute",
                "ec2:ModifyVpcEndpoint",
                "kms:DescribeKey",
                "kms:ListAliases",
                "kms:ListKeyPolicies",
                "kms:ListKeys",
```

```
                "kms:ListRetirableGrants",
                "logs:DescribeLogStreams",
                "logs:GetLogEvents",
                "sns:ListSubscriptions",
                "sns:ListTopics",
                "sns:Publish"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "DocdbSLRSid",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "rds.amazonaws.com"
                }
            }
        },
        {
            "Sid": "DocdbElasticSLRSid",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/docdb-
elastic.amazonaws.com/AWSServiceRoleForDocDB-Elastic",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "docdb-elastic.amazonaws.com"
                }
            }
        }
    ]
}
```

AmazonDocDBElasticReadOnlyAccess

Esta política otorga permisos de solo lectura que permiten a los usuarios ver información del clúster elástico en Amazon DocumentDB. Las entidades principales con esta política asociada no pueden

realizar actualizaciones ni eliminar los recursos existentes, ni pueden crear nuevos recursos de Amazon DocumentDB. Por ejemplo, las entidades principales con estos permisos pueden ver la lista de configuraciones y clústeres asociados a su cuenta, pero no pueden cambiar la configuración ni los ajustes de ningún clúster. Los permisos de esta política se agrupan de la siguiente manera:

- Los permisos de clúster elástico de Amazon DocumentDB le permiten enumerar los recursos del clúster elástico de Amazon DocumentDB, describirlos y obtener información sobre ellos.
- CloudWatch los permisos se utilizan para verificar las métricas del servicio.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "docdb-elastic:ListClusters",
            "docdb-elastic:GetCluster",
            "docdb-elastic:ListClusterSnapshots",
            "docdb-elastic:GetClusterSnapshot",
            "docdb-elastic:ListTagsForResource"
         ],
         "Resource": "*"
      },
      {
         "Effect": "Allow",
         "Action": [
            "cloudwatch:GetMetricData",
            "cloudwatch:ListMetrics",
            "cloudwatch:GetMetricStatistics"
         ],
         "Resource": "*"
      }
   ]
}
```

AmazonDocDBElasticFullAccess

Esta política otorga permisos administrativos que brindan a una entidad principal acceso completo a todas las acciones de Amazon DocumentDB para un clúster elástico de Amazon DocumentDB.

Esta política utiliza AWS etiquetas (https://docs.aws.amazon.com/tag-editor/latest/userguide/tagging.html) dentro de las condiciones para limitar el acceso a los recursos. Si utiliza una secreta, debe estar etiquetada con una clave de etiqueta `DocDBElasticFullAccess` y un valor de etiqueta. Si utiliza una clave administrada por el cliente, debe estar etiquetada con una clave de etiqueta `DocDBElasticFullAccess` y un valor de etiqueta.

Los permisos de esta política se agrupan de la siguiente manera:

- Los permisos de clúster elástico de Amazon DocumentDB permiten todas las acciones de Amazon DocumentDB.
- Algunos de los EC2 permisos de Amazon de esta política son necesarios para validar los recursos aprobados en una solicitud de API. Esto es para garantizar que Amazon DocumentDB pueda utilizar correctamente los recursos para ofrecer y mantener un clúster. El resto de los EC2 permisos de Amazon de esta política permiten a Amazon DocumentDB crear AWS los recursos necesarios para que pueda conectarse a sus clústeres como un punto de enlace de VPC.
- AWS KMS se requieren permisos para que Amazon DocumentDB pueda utilizar la clave pasada para cifrar y descifrar los datos en reposo dentro del clúster elástico de Amazon DocumentDB.

  > **Note**
  >
  > La clave administrada por el cliente debe tener una etiqueta con una clave `DocDBElasticFullAccess` y un valor de etiqueta.

- SecretsManager se requieren permisos para validar un secreto determinado y usarlo para configurar el usuario administrador de los clústeres elásticos de Amazon DocumentDB.

  > **Note**
  >
  > La secreta utilizada debe tener una etiqueta con una clave `DocDBElasticFullAccess` y un valor de etiqueta.

- Se requieren permisos de IAM para crear los roles vinculados al servicio necesarios para la publicación de métricas y registros.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "DocdbElasticSid",
            "Effect": "Allow",
            "Action": [
                "docdb-elastic:CreateCluster",
                "docdb-elastic:UpdateCluster",
                "docdb-elastic:GetCluster",
                "docdb-elastic:DeleteCluster",
                "docdb-elastic:ListClusters",
                "docdb-elastic:CreateClusterSnapshot",
                "docdb-elastic:GetClusterSnapshot",
                "docdb-elastic:DeleteClusterSnapshot",
                "docdb-elastic:ListClusterSnapshots",
                "docdb-elastic:RestoreClusterFromSnapshot",
                "docdb-elastic:TagResource",
                "docdb-elastic:UntagResource",
                "docdb-elastic:ListTagsForResource",
                "docdb-elastic:CopyClusterSnapshot",
                "docdb-elastic:StartCluster",
                "docdb-elastic:StopCluster",
                "docdb-elastic:GetPendingMaintenanceAction",
                "docdb-elastic:ListPendingMaintenanceActions",
                "docdb-elastic:ApplyPendingMaintenanceAction"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "EC2Sid",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateVpcEndpoint",
                "ec2:DescribeVpcEndpoints",
                "ec2:DeleteVpcEndpoints",
                "ec2:ModifyVpcEndpoint",
                "ec2:DescribeVpcAttribute",
                "ec2:DescribeSecurityGroups",
```

```
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeAvailabilityZones",
                "secretsmanager:ListSecrets"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:CalledViaFirst": "docdb-elastic.amazonaws.com"
                }
            }
        },
        {
            "Sid": "KMSSid",
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:DescribeKey",
                "kms:GenerateDataKey"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "kms:ViaService": [
                        "docdb-elastic.*.amazonaws.com"
                    ],
                    "aws:ResourceTag/DocDBElasticFullAccess": "*"
                }
            }
        },
        {
            "Sid": "KMSGrantSid",
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/DocDBElasticFullAccess": "*",
                    "kms:ViaService": [
                        "docdb-elastic.*.amazonaws.com"
```

```
                    ]
                },
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
        },
        {
            "Sid": "SecretManagerSid",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:ListSecretVersionIds",
                "secretsmanager:DescribeSecret",
                "secretsmanager:GetSecretValue",
                "secretsmanager:GetResourcePolicy"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "secretsmanager:ResourceTag/DocDBElasticFullAccess": "*"
                },
                "StringEquals": {
                    "aws:CalledViaFirst": "docdb-elastic.amazonaws.com"
                }
            }
        },
        {
            "Sid": "CloudwatchSid",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:GetMetricData",
                "cloudwatch:ListMetrics",
                "cloudwatch:GetMetricStatistics"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "SLRSid",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/docdb-
elastic.amazonaws.com/AWSServiceRoleForDocDB-Elastic",
```

```
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "docdb-elastic.amazonaws.com"
                }
            }
        }
    ]
}
```

AmazonDocDB- ElasticServiceRolePolicy

No puedes unirte `AmazonDocDBElasticServiceRolePolicy` a tus AWS Identity and Access Management entidades. Esta política está adjunta a un rol vinculado a servicios que permite a Amazon DocumentDB realizar acciones en su nombre. Para obtener más información, consulte Roles vinculados a servicios en clústeres elásticos.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": [
                        "AWS/DocDB-Elastic"
                    ]
                }
            }
        }
    ]
}
```

Amazon DocumentDB actualiza las políticas gestionadas AWS

Cambio	Descripción	Fecha
AmazonDocDBElasticFullAccess, AmazonDocDBConsoleFullAccess - Cambio	Políticas actualizadas para añadir las acciones de mantenimiento pendientes.	11/2/2025
AmazonDocDBElasticFullAccess, AmazonDocDBConsoleFullAccess - Cambio	Se actualizaron las políticas para añadir start/stop agrupar y copiar acciones instantáneas de clústeres.	21/02/2024
AmazonDocDBElasticReadOnlyAccess, AmazonDocDBElasticFullAccess - Cambio	Las políticas se actualizaron para añadir acciones `cloudwatch:GetMetricData` .	21/06/2023
AmazonDocDBElasticReadOnlyAccess: política nueva	Nueva política administrada para los clústeres elásticos de Amazon DocumentDB	8/06/2023
AmazonDocDBElasticFullAccess: política nueva	Nueva política administrada para los clústeres elásticos de Amazon DocumentDB	5/6/2023
AmazonDocDB- ElasticServiceRolePolicy: política nueva	Amazon DocumentDB crea un nuevo rol vinculado al servicio AWS ServiceRoleForDoc DB-Elastic para los clústeres elásticos de Amazon DocumentDB.	30 de noviembre de 2022
AmazonDocDBConsoleFullAccess: cambio	Política actualizada para añadir permisos de clúster elásticos y globales de Amazon DocumentDB.	30/11/2022

Cambio	Descripción	Fecha
AmazonDocDBConsole FullAccess, AmazonDoc DBFullAcceso, AmazonDoc DBReadOnlyAccess: política nueva	Lanzamiento del servicio.	19/1/2017

Permisos de la API de Amazon DocumentDB: referencia de acciones, recursos y condiciones

Use las siguientes secciones como referencia cuando configure Uso de políticas basadas en identidad (políticas de IAM) para Amazon DocumentDB y escriba políticas de permisos que pueda asociar a una identidad de IAM (políticas basadas en identidad).

A continuación se lista cada una de las operaciones de la API de Amazon DocumentDB. En la lista se incluyen las acciones correspondientes para las que puede conceder permisos para realizar la acción, el AWS recurso para el que puede conceder los permisos y las claves de condición que puede incluir para un control de acceso detallado. Las acciones se especifican en el campo `Action` de la política, el valor del recurso en el campo `Resource` de la política y las condiciones en el campo `Condition` de la política. Para obtener más información acerca de las condiciones, consulte Especificación de las condiciones de una política.

Puede utilizar claves AWS de condición amplias en sus políticas de Amazon DocumentDB para expresar las condiciones. Para obtener una lista completa de las claves AWS de ancho, consulte las claves disponibles en la Guía del usuario de IAM.

Puede probar las políticas de IAM con el simulador de política de IAM. Proporciona automáticamente una lista de los recursos y parámetros necesarios para cada AWS acción, incluidas las acciones de Amazon DocumentDB. El simulador de política de IAM determina los permisos necesarios para cada una de las acciones especificadas. Para obtener información sobre el simulador de políticas de IAM, consulte Probar las políticas de IAM con el simulador de políticas de IAM en la Guía del usuario de IAM.

> **Note**
>
> Para especificar una acción, use el prefijo `rds:` seguido del nombre de operación de la API (por ejemplo, `rds:CreateDBInstance`).

A continuación se muestran operaciones de API de Amazon RDS y sus acciones relacionadas, recursos y claves de condición.

Temas

- Acciones de Amazon DocumentDB que admiten permisos de nivel de recursos
- Acciones de Amazon DocumentDB que no admiten permisos de nivel de recursos

Acciones de Amazon DocumentDB que admiten permisos de nivel de recursos

Los permisos a nivel de recursos proporcionan la capacidad de especificar qué usuarios pueden realizar acciones en qué recursos. Amazon DocumentDB admite parcialmente los permisos de nivel de recursos. Esto significa que, en algunas acciones de Amazon DocumentDB, puede determinar cuándo se permite utilizarlas a los usuarios en función de si se cumplen una serie de condiciones o de los recursos concretos que pueden utilizar los usuarios. Por ejemplo, puede conceder a los usuarios permiso para modificar solo instancias específicas.

A continuación se muestran operaciones de API de Amazon DocumentDB y sus acciones relacionadas, recursos y claves de condición.

> **Note**
>
> En determinadas características de administración, Amazon DocumentDB utiliza una tecnología operativa que comparte con Amazon RDS. Para obtener más información sobre los permisos de Amazon DocumentDB, consulte Actions, resources, and condition keys for Amazon RDS en la Referencia de autorización de servicios.

Acciones y operaciones de la API de Amazon DocumentDB	Recursos	Claves de condición
AddTagsToResource rds:AddTagsToResource	Instancia arn:aws:rds: *region*:*account-id* :db:*db-instance-name*	rds:db-tag
	Grupo de subredes arn:aws:rds: *region*:*account-id* :subgrp:*subnet-group-name*	rds:subgrp-tag
ApplyPendingMaintenanceAction rds:ApplyPendingMaintenanceAction	Instancia arn:aws:rds: *region*:*account-id* :db:*db-instance-name*	rds:db-tag
Copiar DBCluster instantánea rds:CopyDBClusterSnapshot	Instantánea de clúster arn:aws:rds: *region*:*account-id* :cluster-snapshot: *cluster-snapshot-name*	rds:cluster-snapshot-tag
CrearDBCluster rds:CreateDBCluster	Clúster arn:aws:rds: *region*:*account-id* :cluster: *db-cluster-name*	rds:cluster-tag
	Grupo de parámetros del clúster	rds:cluster-pg-tag

Acciones y operaciones de la API de Amazon DocumentDB	Recursos	Claves de condición
	arn:aws:rds: *region*:*account-id* :cluster-pg: *cluster-parameter-group-name*	
	Grupo de subredes arn:aws:rds: *region*:*account-id* :subgrp:*subnet-group-name*	rds:subgrp-tag
CrearDBClusterParameterGroup rds:CreateDBClusterParameterGroup	Grupo de parámetros del clúster arn:aws:rds: *region*:*account-id* :cluster-pg: *cluster-parameter-group-name*	rds:cluster-pg-tag
Crear DBCluster instantánea rds:CreateDBClusterSnapshot	Clúster arn:aws:rds: *region*:*account-id* :cluster: *db-cluster-name*	rds:cluster-tag
	Instantánea de clúster arn:aws:rds: *region*:*account-id* :cluster-snapshot: *cluster-snapshot-name*	rds:cluster-snapshot-tag
CrearDBInstance rds:CreateDBInstance	Instancia arn:aws:rds: *region*:*account-id* :db:*db-instance-name*	rds:DatabaseClass rds:db-tag

Acciones y operaciones de la API de Amazon DocumentDB	Recursos	Claves de condición
	Clúster arn:aws:rds: *region*:*account-id* :cluster: *db-cluster-name*	rds:cluster-tag
Crear DBSubnet grupo rds:CreateDBSubnetGroup	Grupo de subredes arn:aws:rds: *region*:*account-id* :subgrp:*subnet-group-name*	rds:subgrp-tag
DeleteDBInstance rds:DeleteDBInstance	Instancia arn:aws:rds: *region*:*account-id* :db:*db-instance-name*	rds:db-tag
Eliminar DBSubnet grupo rds:DeleteDBSubnetGroup	Grupo de subredes arn:aws:rds: *region*:*account-id* :subgrp:*subnet-group-name*	rds:subgrp-tag
DescribirDBClusterParameterGroups rds:DescribeDBClusterParameterGroups	Grupo de parámetros del clúster arn:aws:rds: *region*:*account-id* :cluster-pg: *cluster-parameter-group-name*	rds:cluster-pg-tag

Acciones y operaciones de la API de Amazon DocumentDB	Recursos	Claves de condición
Describa DBCluster los parámetros rds:DescribeDBClusterParameters	Grupo de parámetros del clúster arn:aws:rds: *region*:*account-id* :cluster-pg: *cluster-parameter-group-name*	rds:cluster-pg-tag
DescribirDBClusters rds:DescribeDBClusters	Clúster arn:aws:rds: *region*:*account-id* :cluster: *db-cluster-instance-name*	rds:cluster-tag
DescribirDBClusterSnapshotAttributes rds:DescribeDBClusterSnapshotAttributes	Instantánea de clúster arn:aws:rds: *region*:*account-id* :cluster-snapshot: *cluster-snapshot-name*	rds:cluster-snapshot-tag
Describa DBSubnet los grupos rds:DescribeDBSubnetGroups	Grupo de subredes arn:aws:rds: *region*:*account-id* :subgrp:*subnet-group-name*	rds:subgrp-tag
DescribePendingMaintenanceActions rds:DescribePendingMaintenanceActions	Instancia arn:aws:rds: *region*:*account-id* :db:*db-instance-name*	rds:DatabaseClass rds:db-tag

Acciones y operaciones de la API de Amazon DocumentDB	Recursos	Claves de condición
Conmutación por error DBCluster rds:FailoverDBCluster	Clúster arn:aws:rds: *region*:*account-id* :cluster: *db-cluster-instance-name*	rds:cluster-tag
ListTagsForResource rds:ListTagsForResource	Instancia arn:aws:rds: *region*:*account-id* :db:*db-instance-name*	rds:db-tag
	Grupo de subredes arn:aws:rds: *region*:*account-id* :subgrp:*subnet-group-name*	rds:subgrp-tag
ModifyDBCluster rds:ModifyDBCluster	Clúster arn:aws:rds: *region*:*account-id* :cluster: *db-cluster-name*	rds:cluster-tag
	Grupo de parámetros del clúster arn:aws:rds: *region*:*account-id* :cluster-pg: *cluster-parameter-group-name*	rds:cluster-pg-tag
ModifyDBClusterParameterGroup rds:ModifyDBClusterParameterGroup	Grupo de parámetros del clúster arn:aws:rds: *region*:*account-id* :cluster-pg: *cluster-parameter-group-name*	rds:cluster-pg-tag

Acciones y operaciones de la API de Amazon DocumentDB	Recursos	Claves de condición
ModifyDBClusterSnapshotAttribute rds:ModifyDBClusterSnapshotAttribute	Instantánea de clúster arn:aws:rds: *region*:*account-id* :cluster-snapshot: *cluster-snapshot-name*	rds:cluster-snapshot-tag
ModifyDBInstance rds:ModifyDBInstance	Instancia arn:aws:rds: *region*:*account-id* :db:*db-instance-name*	rds:DatabaseClass rds:db-tag
Reiniciar DBInstance rds:RebootDBInstance	Instancia arn:aws:rds: *region*:*account-id* :db:*db-instance-name*	rds:db-tag
RemoveTagsFromResource rds:RemoveTagsFromResource	Instancia arn:aws:rds: *region*:*account-id* :db:*db-instance-name*	rds:db-tag
	Grupo de subredes arn:aws:rds: *region*:*account-id* :subgrp:*subnet-group-name*	rds:subgrp-tag
RestablecerDBClusterParameterGroup rds:ResetDBClusterParameterGroup	Grupo de parámetros del clúster arn:aws:rds: *region*:*account-id* :cluster-pg: *cluster-parameter-group-name*	rds:cluster-pg-tag

Acciones y operaciones de la API de Amazon DocumentDB	Recursos	Claves de condición
RestaurarDBClusterFromSnapshot rds:RestoreDBClusterFromSnapshot	Clúster arn:aws:rds: *region*:*account-id* :cluster: *db-cluster-instance-name*	rds:cluster-tag
	Instantánea de clúster arn:aws:rds: *region*:*account-id* :cluster-snapshot: *cluster-snapshot-name*	rds:cluster-snapshot-tag
RestaurarDBClusterToPointInTime rds:RestoreDBClusterToPointInTime	Clúster arn:aws:rds: *region*:*account-id* :cluster: *db-cluster-instance-name*	rds:cluster-tag
	Grupo de subredes arn:aws:rds: *region*:*account-id* :subgrp:*subnet-group-name*	rds:subgrp-tag

Acciones de Amazon DocumentDB que no admiten permisos de nivel de recursos

Puede usar todas las acciones de Amazon DocumentDB de una política de IAM para conceder o denegar permiso a los usuarios para utilizar esa acción. Sin embargo, no todas las acciones de Amazon DocumentDB admiten permisos de nivel de recursos, que le permiten especificar los recursos en los que se puede realizar una acción. Las siguientes acciones de la API de Amazon DocumentDB no admiten actualmente permisos de nivel de recursos. Por lo tanto, para usar estas acciones en una política de IAM, debe conceder permiso a los usuarios para utilizar todos los recursos para la acción; para ello, emplee en su instrucción un carácter comodín * para el elemento `Resource`.

- `rds:DescribeDBClusterSnapshots`
- `rds:DescribeDBInstances`

Autenticación mediante la identidad de IAM

Los usuarios y las aplicaciones de Amazon DocumentDB pueden utilizar los usuarios y roles de IAM para autenticarse en un clúster de Amazon DocumentDB. La autenticación de IAM de Amazon DocumentDB es un método de autenticación sin contraseña. Además, las aplicaciones cliente no envían los secretos de las contraseñas al clúster de Amazon DocumentDB cuando utilizan roles o usuarios de IAM. En su lugar, las conexiones de los clientes se autentican mediante AWS STS con tokens de seguridad temporales. Las aplicaciones y los usuarios no administrativos ahora pueden usar el mismo ARN de identidad de IAM al conectarse a distintos clústeres de Amazon DocumentDB y a otros servicios de AWS.

También puede optar por utilizar la autenticación basada en contraseña y la autenticación de IAM para autenticar los usuarios y las aplicaciones en un clúster de Amazon DocumentDB. La autenticación de IAM solo está disponible en la versión 5.0 del clúster basado en instancias de Amazon DocumentDB. El usuario principal de Amazon DocumentDB no admite la autenticación de IAM mediante ARN de identidad de IAM.

> **Note**
>
> El usuario principal solo se puede autenticar mediante la autenticación basada en contraseñas existente.

Temas

- Introducción a la autenticación mediante roles y usuarios de IAM
- Configuración de tipos de cómputo de AWS para autenticarse en Amazon DocumentDB mediante AWS IAM
- Supervisión de solicitudes de autenticación de IAM
- Uso de la autenticación de IAM
- Controladores compatibles con IAM
- Preguntas frecuentes sobre la autenticación de identidad de IAM

Introducción a la autenticación mediante roles y usuarios de IAM

Los usuarios y roles de Amazon DocumentDB con identidades de IAM se crean y administran en una base de datos de `$external`.

Creación de un usuario

Conéctese como usuario principal y, a continuación, cree un usuario y un rol de IAM:

```
use $external;
db.createUser(
    {
        user: "arn:aws:iam::123456789123:user/iamuser",
        mechanisms: ["MONGODB-AWS"],
        roles: [ { role: "readWrite", db: "readWriteDB" } ]
    }
);
```

Como alternativa, agregue un usuario de Amazon DocumentDB con un rol de IAM:

```
use $external;
db.createUser(
    {
        user: "arn:aws:iam::123456789123:role/iamrole",
        mechanisms: ["MONGODB-AWS"],
        roles: [ { role: "readWrite", db: "readWriteDB" } ]
    }
);
```

Modificación de un usuario o rol de IAM

Modificación de un usuario de IAM existente:

```
use $external;
db.updateUser(
  "arn:aws:iam::123456789123:user/iamuser",
  {
    roles: [ { role: "read", db: "readDB" } ]
  }
);
```

Modificación de un rol de IAM existente:

```
use $external;
db.updateUser(
  "arn:aws:iam::123456789123:role/iamrole",
  {
    roles: [ { role: "read", db: "readDB" } ]
  }
);
```

Concesión o revocación de roles de un usuario de IAM:

```
use $external;
db.grantRolesToUser(
  "arn:aws:iam::123456789123:user/iamuser",
  [ { db: "admin", role: "readWriteAnyDatabase" } ]
);
```

```
use $external;
db.revokeRolesFromUser(
  "arn:aws:iam::123456789123:user/iamuser",
  [ { db: "admin", role: "readWriteAnyDatabase" } ]
);
```

Concesión o revocación de roles de un rol de IAM:

```
use $external;
db.grantRolesToUser(
  "arn:aws:iam::123456789123:user/iamrole",
  [ { db: "admin", role: "readWriteAnyDatabase" } ]
);
```

```
use $external;
db.revokeRolesFromUser(
  "arn:aws:iam::123456789123:user/iamrole",
  [ { db: "admin", role: "readWriteAnyDatabase" } ]
);
```

Eliminación de un usuario o un rol de IAM

Eliminación de un usuario de IAM existente:

```
use $external;
db.dropUser("arn:aws:iam::123456789123:user/iamuser");
```

Eliminación de un rol de IAM existente:

```
use $external;
db.dropUser("arn:aws:iam::123456789123:role/iamrole");
```

Configuración de un URI de conexión para autenticarse mediante AWS IAM

Para autenticarse mediante AWS IAM, utilice los siguientes parámetros de URI: `authSource` como `$external` y `authMechanism` como `MONGODB-AWS`. Si utiliza un usuario de IAM, los campos de nombre de usuario y contraseña se sustituyen por una clave de acceso y una clave secreta, respectivamente. Si asume un rol de IAM asociado al entorno en el que se encuentra (por ejemplo, función AWS Lambda, instancia de Amazon EC2). No es necesario pasar ninguna credencial de manera específica al autenticarse mediante el mecanismo `MONGODB-AWS`. Si utiliza controladores de MongoDB que admiten el mecanismo de autenticación `MONGODB-AWS`, los controladores también tienen la capacidad de recuperar las credenciales del rol de IAM de la instancia de procesamiento (por ejemplo, Amazon EC2, la función de Lambda y otros). En el siguiente ejemplo, se utiliza un shell de mongo para autenticarse con `MONGODB-AWS` mediante el paso manual de una clave de acceso y una clave secreta (de un usuario de IAM) para demostrar la autenticación en Amazon DocumentDB.

En el siguiente ejemplo, se utiliza código Python para autenticarse con `MONGODB-AWS` sin pasar ninguna credencial de forma explícita (mediante un rol de IAM asociado al entorno) para demostrar la autenticación en Amazon DocumentDB.

```
##Create a MongoDB client, open a connection to Amazon DocumentDB using an IAM role
    client = pymongo.MongoClient('mongodb://<DocDBEndpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false&authSource=
%24external&authMechanism=MONGODB-AWS')
```

En el siguiente ejemplo, se utiliza un shell de mongo para autenticarse con el mecanismo `MONGODB-AWS` mediante el paso manual de una clave de acceso y una clave secreta (de un usuario de IAM) para demostrar la autenticación en Amazon DocumentDB.

```
$ mongo 'mongodb://<access_key>:<secret_key>@<cluster_endpoint>:<db_port>/test?
authSource=%24external&authMechanism=MONGODB-AWS'
```

En el siguiente ejemplo, se utiliza un shell de mongo para autenticarse con `MONGODB-AWS` sin pasar ninguna credencial de forma explícita (mediante un rol de IAM asociado al entorno) para demostrar la autenticación en Amazon DocumentDB.

```
$ mongo 'mongodb://<cluster_endpoint>:<db_port>/test?authSource=
%24external&authMechanism=MONGODB-AWS'
```

Configuración de tipos de cómputo de AWS para autenticarse en Amazon DocumentDB mediante AWS IAM

Uso de Amazon EC2/AWS Lambda/AWS Fargate

Amazon EC2 usa las siguientes variables de entorno. Si tiene un rol de IAM asociado a la instancia de EC2 o un rol de IAM de ejecución asociado a una función de Lambda o una tarea de Amazon ECS, estas variables se rellenan automáticamente y el controlador puede obtener estos valores del entorno:

```
AWS_ACCESS_KEY_ID
AWS_SECRET_ACCESS_KEY
AWS_SESSION_TOKEN
```

Para obtener información sobre cómo usar las variables de entorno, consulte Utilice variables de entorno de Lambda en la Guía para desarrolladores de AWS Lambda.

Uso de Amazon EKS

Al asignar un rol a los pods de Amazon Elastic Kubernetes Service (Amazon EKS), se configurarán automáticamente las dos variables de entorno siguientes:

```
AWS_WEB_IDENTITY_TOKEN_FILE - path of web identity token file
AWS_ROLE_ARN - Name of IAM role to connect with
```

Con la ayuda de estas variables, asuma manualmente el rol a partir del código mediante la llamada del AWS SDK para `AssumeRoleWithWebIdentity`:

- Omita el parámetro `ProviderID`.
- Busque el valor del parámetro `WebIdentityToken` en el archivo descrito en la variable de entorno `AWS_WEB_IDENTITY_TOKEN_FILE`.

Para obtener más información en Amazon EKS, consulte ¿Qué es Amazon EKS? en la Guía del usuario de Amazon EKS.

Supervisión de solicitudes de autenticación de IAM

Uso de la auditoría de Amazon DocumentDB

Vaya a la carpeta de registros de auditoría de Amazon CloudWatch y utilice diferentes patrones de búsqueda para obtener los registros de la autenticación de IAM. Por ejemplo, utilice `{ $.param.mechanism = "MONGODB-AWS" }` como patrón de búsqueda para “Buscar en todos los flujos de registro”.

Para obtener más información sobre los eventos compatibles en la auditoría, consulte Auditoría de eventos de Amazon DocumentDB.

Uso de métricas de Amazon CloudWatch

`StsGetCallerIdentityCalls`: esta métrica muestra el número de llamadas `GetCallerIdentity` que hace una instancia de Amazon DocumentDB al punto de conexión regionalizado AWS Security Token Service (AWS STS). Consulte la especificación de autenticación de `MONGODB-AWS` para saber por qué las instancias de base de datos deben hacer llamadas `GetCallerIdentity` a STS.

Uso de la autenticación de IAM

Si no desea administrar el nombre de usuario y la contraseña de su propia base de datos, puede utilizar la autenticación de IAM. La autenticación de IAM solo está disponible en la versión 5.0 del clúster basado en instancias de Amazon DocumentDB.

La autenticación de IAM depende del servicio STS. Le recomendamos que evalúe si puede reducir la velocidad de conexión si utiliza la autenticación de IAM para la conexión y obtiene una excepción de limitación del STS.

Para obtener más información acerca de las cuotas de IAM, consulte IAM y cuotas de AWS STS en la Guía del usuario de IAM.

Controladores compatibles con IAM

Los controladores compatibles con Amazon DocumentDB 5.0 y el mecanismo de autenticación de `MONGODB-AWS` deberían funcionar con la implementación de autenticación de IAM en Amazon DocumentDB.

> **Important**
>
> Existe una limitación conocida con los controladores de Node.js anteriores a la versión 6.13.1, ya que Amazon DocumentDB no los admite actualmente para la autenticación de identidad de IAM. Los controladores y las herramientas de Node.js que utilizan el controlador Node.js (por ejemplo, mongosh) deben actualizarse para utilizar el controlador Node.js, versión 6.13.1 o posterior.

Preguntas frecuentes sobre la autenticación de identidad de IAM

Hay alguna muestra que pueda consultar?

Consulte estas páginas para ver ejemplos de casos de uso y configuraciones:

- Cómo los usuarios humanos pueden autenticarse en Amazon DocumentDB mediante usuarios y roles de IAM
- Autenticación sin contraseña en Amazon DocumentDB mediante roles de IAM

Recibo un error al usar mi controlador de Python: “pymongo.errors.ConfigurationError: MONGODB-AWS authentication requires pymongo-auth-aws”. Cómo puedo resolver esto?

Asegúrese de utilizar la siguiente declaración al instalar el controlador de Python con la autenticación de IAM:

```
pip install 'pymongo[aws]'
```

Esto instalará las dependencias adicionales de AWS necesarias para que funcione la autenticación de IAM.

Se interrumpirá mi conexión cuando caduquen las credenciales temporales de mi rol de IAM?

No, las credenciales de IAM temporales solo se utilizan para establecer la conexión y la autenticación. A continuación, todas las autorizaciones adicionales se producen en el clúster de Amazon DocumentDB. Incluso si las credenciales de IAM cambian o caducan, la conexión no se interrumpirá ni quedará obsoleta.

Administración de usuarios de Amazon DocumentDB

En Amazon DocumentDB, los usuarios se autentican en un clúster junto con una contraseña. Cada clúster tiene credenciales de inicio de sesión principales que se establecen durante la creación del clúster.

> **Note**
>
> Todos los nuevos usuarios creados antes del 26 de marzo de 2020 han recibido los roles `dbAdminAnyDatabase`, `readWriteAnyDatabase`, y `clusterAdmin`. Se recomienda que vuelva a evaluar todos los usuarios y modifique los roles según sea necesario para aplicar los privilegios mínimos para todos los usuarios de los clústeres.
> Para obtener más información, consulte Acceso a la base de datos mediante el control de acceso basado en roles.

Usuario principal y usuario **`serviceadmin`**

Un clúster recién creado de Amazon DocumentDB tiene dos usuarios: el usuario principal y el usuario `serviceadmin`.

El usuario principal es un usuario único con privilegios que puede realizar tareas administrativas y crear usuarios adicionales con roles. Cuando se conecta a un clúster de Amazon DocumentDB por primera vez, debe autenticarse con las credenciales de inicio de sesión principales. El usuario principal recibe estos permisos administrativos para un clúster de Amazon DocumentDB cuando se crea ese clúster y se le concede el rol de `root`.

El usuario `serviceadmin` se crea implícitamente cuando se crea el clúster. Cada clúster Amazon DocumentDB tiene un usuario `serviceadmin` que proporciona a AWS la capacidad de administrar su clúster. No puede iniciar sesión como, ni eliminarlo, cambiarlo de nombre, cambiar su contraseña o cambiar los permisos para `serviceadmin`. Cualquier intento de realizar una de estas operaciones producirá un error.

> **Note**
>
> El principal y los usuarios `serviceadmin` de un clúster de Amazon DocumentDB no se pueden eliminar y el rol de `root` para el usuario principal no se puede revocar.

Si olvida su contraseña de usuario principal, puede restablecerla con la Consola de administración de AWS o la AWS CLI.

Creación de usuarios adicionales

Después de conectarse como usuario principal (o cualquier usuario que tenga el rol `createUser`), puede crear un nuevo usuario, como se muestra a continuación.

```
db.createUser(
    {
        user: "sample-user-1",
        pwd: "password123",
        roles:
            [{"db":"admin", "role":"dbAdminAnyDatabase" }]
    }
)
```

Para ver los detalles del usuario, puede utilizar el comando `show users` de la siguiente manera. También puede eliminar usuarios con el comando `dropUser`. Para obtener más información, consulte Comandos comunes.

```
show users
{
    "_id" : "serviceadmin",
    "user" : "serviceadmin",
    "db" : "admin",
    "roles" : [
     {
            "role" : "root",
            "db" : "admin"
        }
    ]
},

{
    "_id" : "myPrimaryUser",
    "user" : "myPrimaryUser",
    "db" : "admin",
    "roles" : [
```

```
     {
            "role" : "root",
            "db" : "admin"
        }
    ]
},

{
    "_id" : "sample-user-1",
    "user" : "sample-user-1",
    "db" : "admin",
    "roles" : [
     {
            "role" : "dbAdminAnyDatabase",
            "db" : "admin"
     }
    ]
}
```

En este ejemplo, el nuevo usuario `sample-user-1` se atribuye a la base de datos `admin`. Esto se aplica siempre en el caso de un usuario nuevo. Amazon DocumentDB no tiene el concepto de una `authenticationDatabase` y, por lo tanto, toda la autenticación se realiza en el contexto de la base de datos `admin`.

Al crear usuarios, si omite el campo db al especificar el rol, Amazon DocumentDB atribuirá implícitamente el rol a la base de datos en la que se está emitiendo la conexión. Por ejemplo, si la conexión se emite contra la base de datos `sample-database` y ejecuta el siguiente comando, el usuario `sample-user-2` se creará en la base de datos del `admin` y tendrá permisos `readWrite` para la base de datos `sample-database`.

```
db.createUser(
    {
        user: "sample-user-2",
        pwd: "password123",
        roles:
            ["readWrite"]
    }
)
```

La creación de usuarios con roles cuyo ámbito se encuentra en todas las bases de datos (por ejemplo, `readInAnyDatabase`) requiere que se encuentre en el contexto de la base de datos `admin` al crear el usuario o que indique explícitamente la base de datos para el rol al crear el usuario.

Para cambiar el contexto de la base de datos, puede utilizar el siguiente comando.

```
use admin
```

Para obtener más información sobre el control de acceso basado en roles y la aplicación de privilegios mínimos entre los usuarios del clúster, consulte Acceso a la base de datos mediante el control de acceso basado en roles.

Rotación automática de contraseñas para Amazon DocumentDB

Con AWS Secrets Manager, puede reemplazar las credenciales codificadas en el código (incluidas contraseñas), con una llamada a la API de Secrets Manager para recuperar el secreto mediante programación. Esto ayuda a garantizar la integridad del secreto si alguien examina el código, dado que el secreto sencillamente no está allí. Asimismo, puede configurar Secrets Manager para rotar el secreto automáticamente de acuerdo con la programación que especifique. Esto le permite reemplazar secretos a largo plazo con secretos a corto plazo, lo que contribuye a reducir significativamente el riesgo de peligro.

Con Secrets Manager, puede rotar automáticamente las contraseñas de Amazon DocumentDB (es decir, secretos) mediante una función de AWS Lambda que Secrets Manager proporciona.

Para obtener más información acerca AWS Secrets Manager y la integración nativa con Amazon DocumentDB, consulte lo siguiente:

- Blog: How to rotate Amazon DocumentDB and Amazon Redshift credentials in AWS Secrets Manager
- ¿Qué es Secrets Manager de AWS?
- Rotar secretos de AWS Secrets Manager
- Credenciales de Amazon DocumentDB en Secrets Manager

Acceso a la base de datos mediante el control de acceso basado en roles

Puede restringir el acceso a las acciones que los usuarios pueden realizar en bases de datos mediante el control de acceso basado en roles (RBAC) en Amazon DocumentDB (con compatibilidad con MongoDB). RBAC funciona otorgando uno o más roles a un usuario. Estos roles determinan las operaciones que un usuario puede realizar en los recursos de la base de datos. Actualmente, Amazon DocumentDB admite tanto roles integrados que se centran en el nivel de base de datos, como `read`, `readWrite`, `readAnyDatabase`, `clusterAdmin`, y roles definidos por el usuario que se pueden limitar a acciones específicas y recursos granulares, como colecciones, en función de sus requisitos.

Los casos de uso comunes para RBAC incluyen la imposición de privilegios mínimos mediante la creación de usuarios con acceso de sólo lectura a las bases de datos o colecciones en un clúster, y diseños de aplicaciones multitenant que permiten a un solo usuario acceder a una base de datos determinada o colección en un clúster.

> **Note**
>
> Todos los nuevos usuarios creados antes del 26 de marzo de 2020 han recibido los roles `dbAdminAnyDatabase`, `readWriteAnyDatabase`, y `clusterAdmin`. Se recomienda volver a evaluar todos los usuarios existentes y modificar los roles según sea necesario para aplicar los privilegios mínimos para los clústeres.

Temas

- Conceptos de RBAC
- Introducción a los roles integrados de RBAC
- Introducción a los roles definidos por el usuario de RBAC
- Conexión a Amazon DocumentDB como un usuario
- Comandos comunes
- Diferencias funcionales
- Límites de las s
- Acceso a la base de datos mediante el control de acceso basado en roles

Conceptos de RBAC

Los siguientes son términos y conceptos importantes relacionados con el control de acceso basado en roles. Para obtener más información sobre los usuarios de Amazon DocumentDB, consulteAdministración de usuarios de Amazon DocumentDB.

- Usuario: entidad individual que puede autenticarse en la base de datos y realizar operaciones.
- Contraseña: secreto que se utiliza para autenticar al usuario.
- Rol: autoriza a un usuario a realizar acciones en una o más bases de datos.
- Base de datos de administración: la base de datos en la que se almacenan los usuarios y en la que se autoriza su uso.
- Base de datos (**db**): el espacio de nombres dentro de los clústeres que contiene colecciones para almacenar documentos.

El comando siguiente crea un usuario llamado `sample-user`.

```
db.createUser({user: "sample-user", pwd: "abc123", roles: [{role: "read", db: "sample-database"}]})
```

En este ejemplo:

- `user: "sample-user"`: indica el nombre de usuario.
- `pwd: "abc123"`: indica la contraseña del usuario.
- `role: "read", "db: "sample-database"`: indica que el `sample-user` de usuario tendrá permisos de lectura en `sample-database`.



El siguiente ejemplo muestra el resultado después de obtener el usuario `sample-user` con `db.getUser(sample-user)`. En este ejemplo, el usuario `sample-user` reside en la base de datos del `admin` pero tiene el rol de lectura para la base de datos `sample-database`.



Al crear usuarios, si omite el campo db al especificar el rol, Amazon DocumentDB atribuirá implícitamente el rol a la base de datos en la que se está emitiendo la conexión. Por ejemplo, si la conexión se emite contra la base de datos `sample-database` y ejecuta el siguiente comando, el usuario `sample-user` se creará en la base de datos del `admin` y tendrá permisos `readWrite` para la base de datos `sample-database`.

```
db.createUser({user: "sample-user", pwd: "abc123", roles: ["readWrite"]})
```

La salida de esta operación será similar a lo que se indica a continuación.

```
{
   "user":"sample-user",
   "roles":[
      {
         "db":"sample-database",
         "role":"readWrite"
      }
   ]
}
```

La creación de usuarios con roles cuyo ámbito se encuentra en todas las bases de datos (por ejemplo, `readAnyDatabase`) requiere que esté en el contexto de la base de datos de `admin` al crear el usuario o que indique explícitamente la base de datos para el rol al crear el usuario. Para emitir comandos contra la base de datos del `admin`, puede utilizar el comando `use admin`. Para obtener más información, consulte Comandos comunes.

Introducción a los roles integrados de RBAC

Para ayudarle a comenzar con el control de acceso basado en roles, esta sección le guía a través de un escenario de ejemplo de aplicación de privilegios mínimos mediante la creación de roles para tres usuarios con funciones de trabajo diferentes.

- `user1` es un nuevo administrador que necesita poder ver y acceder a todas las bases de datos de un clúster.
- `user2` es un nuevo empleado que necesita acceso a una sola base de datos, `sample-database-1`, en ese mismo clúster.
- `user3` es un empleado existente que necesita ver y tener acceso a una base de datos diferente, `sample-database-2`, a la que no tenían acceso antes, en el mismo clúster.

En un momento posterior, tanto `user1` como `user2` abandonan la empresa y por lo tanto su acceso debe ser revocado.

Para crear usuarios y otorgar roles, el usuario con el que se autentique en el clúster debe tener un rol asociado que pueda realizar acciones para `createUser` y `grantRole`. Por ejemplo, los roles `admin` y `userAdminAnyDatabase` pueden otorgar tales habilidades, por ejemplo. Para ver las acciones por rol, consulte Acceso a la base de datos mediante el control de acceso basado en roles.

> **Note**
>
> En Amazon DocumentDB, todas las operaciones de usuario y rol (por ejemplo, `create`, `get`, `drop`, `grant`, `revoke`, etc.) se realizan implícitamente en la base de datos de `admin`, independientemente de que se estén ejecutando o no comandos contra la base de datos `admin`.

En primer lugar, para comprender cuáles son los usuarios y roles actuales en el clúster, puede ejecutar el comando `show users`, como en el ejemplo siguiente. Verá dos usuarios `serviceadmin` y el usuario principal para el clúster. Estos dos usuarios siempre existen y no se pueden eliminar. Para obtener más información, consulte Administración de usuarios de Amazon DocumentDB.

```
show users
```

Para `user1`, cree un rol con acceso de lectura y escritura a todas las bases de datos de todo el clúster con el siguiente comando.

```
db.createUser({user: "user1", pwd: "abc123", roles: [{role: "readWriteAnyDatabase", db:
 "admin"}]})
```

La salida de esta operación será similar a lo que se indica a continuación.

```
{
   "user":"user1",
   "roles":[
      {
         "role":"readWriteAnyDatabase",
         "db":"admin"
      }
   ]
}
```

Para `user2`, cree un rol con acceso de sólo lectura a la base de datos `sample-database-1` con el siguiente comando.

```
db.createUser({user: "user2", pwd: "abc123", roles: [{role: "read", db: "sample-
database-1"}]})
```

La salida de esta operación será similar a lo que se indica a continuación.

```
{
   "user":"user2",
   "roles":[
      {
         "role":"read",
         "db":"sample-database-1"
      }
   ]
}
```

Para simular el escenario en que `user3` es un usuario existente, primero cree el usuario `user3` y a continuación asigne un nuevo rol a `user3`.

```
db.createUser({user: "user3", pwd: "abc123", roles: [{role: "readWrite", db: "sample-
database-1"}]})
```

La salida de esta operación será similar a lo que se indica a continuación.

```
{
   "user":"user3",
   "roles":[
      {
         "role":"readWrite",
         "db":"sample-database-1"
      }
   ]
}
```

Ahora que se ha creado el usuario `user3`, asigne a `user3` el rol `read` a `sample-database-2`.

```
db.grantRolesToUser("user3", [{role: "read", db: "sample-database-2"}])
```

Por último, tanto `user1` como `user2` abandonan la empresa y su acceso al clúster debe revocarse. Puede hacer esto dejando caer a los usuarios, de la siguiente manera.

```
db.dropUser("user1")
db.dropUser("user2")
```

Para asegurarse de que todos los usuarios tienen los roles adecuados, puede enumerar todos los usuarios con el siguiente comando.

```
show users
```

La salida de esta operación será similar a lo que se indica a continuación.

```
{
   "_id":"serviceadmin",
   "user":"serviceadmin",
   "db":"admin",
   "roles":[
      {
         "db":"admin",
         "role":"root"
```

```
      }
   ]
}
{
   "_id":"master-user",
   "user":"master-user",
   "db":"admin",
   "roles":[
      {
         "db":"admin",
         "role":"root"
      }
   ]
}
{
   "_id":"user3",
   "user":"user3",
   "db":"admin",
   "roles":[
      {
         "db":"sample-database-2",
         "role":"read"
      },
      {
         "db":"sample-database-1",
         "role":"readWrite"
      }
   ]
}
```

Introducción a los roles definidos por el usuario de RBAC

Para ayudarle a comenzar con roles definidos por el usuario, esta sección le guía a través de un escenario de ejemplo de aplicación de privilegios mínimos mediante la creación de roles para tres usuarios con funciones distintas.

En este ejemplo, se aplica lo siguiente:

- `user1` es un nuevo administrador que necesita poder ver y acceder a todas las bases de datos de un clúster.
- `user2` es un nuevo empleado que necesita acceso a la acción ´encontrar´ en una sola base de datos, `sample-database-1`, en ese mismo clúster.

- `user3` es un empleado existente que necesita ver y tener acceso a una colección específica, col2 en una base de datos distinta, `sample-database-2` a la que no tenía acceso antes, en el mismo clúster.
- Para `user1`, cree un rol con acceso de lectura y escritura a todas las bases de datos de todo el clúster con el siguiente comando.

```
db.createUser(
 {
     user: "user1", pwd: "abc123",
     roles: [{role: "readWriteAnyDatabase", db: "admin"}]
 }
 )
```

La salida de esta operación será similar a lo que se indica a continuación.

```
{
   "user":"user1",
   "roles":[
      {
         "role":"readWriteAnyDatabase",
         "db":"admin"
      }
   ]
}
```

Para `user2`, cree un rol con privilegios de “búsqueda” para todas las colecciones de la base de datos `sample-database-1` con el siguiente comando. Tenga en cuenta que este rol garantizaría que los usuarios asociados solo puedan ejecutar consultas de búsqueda.

```
db.createRole(
{
    role: "findRole",
    privileges: [
    {
        resource: {db: "sample-database-1", collection: ""}, actions: ["find"]
    }],
    roles: []
}
)
```

La salida de esta operación será similar a lo que se indica a continuación.

```
{
   "role":"findRole",
   "privileges":[
      {
         "resource":{
            "db":"sample-database-1",
            "collection":""
         },
         "actions":[
            "find"
         ]
      }
   ],
   "roles":[

   ]
}
```

A continuación, cree el usuario (`user2`) y adjunte el rol `findRole` creado recientemente al usuario.

```
db.createUser(
{
    user: "user2",
    pwd: "abc123",
    roles: []
})

 db.grantRolesToUser("user2",["findRole"])
```

Para simular el escenario en que `user3` es un usuario existente, primero cree el usuario `user3` y a continuación asigne un nuevo rol denominado collectionRole a `user3`, algo que haremos en el próximo paso.

Ahora puede asignar un nuevo rol al `user3`. Este nuevo rol permitirá al `user3` insertar, actualizar, eliminar y acceder a una colección específica col2 en la `sample-database-2`.

```
db.createUser(
{
    user: "user3",
```

```
    pwd: "abc123",
    roles: []
})

db.createRole(
{
    role: "collectionRole",
    privileges: [
    {
        resource: {db: "sample-database-2", collection: "col2"}, actions: ["find",
 "update", "insert", "remove"]
    }],
    roles: []
}
)
```

La salida de esta operación será similar a lo que se indica a continuación.

```
{
   "role":"collectionRole",
   "privileges":[
      {
         "resource":{
            "db":"sample-database-2",
            "collection":"col2"
         },
         "actions":[
            "find",
            "update",
            "insert",
            "remove"
         ]
      }
   ],
   "roles":[

   ]
}
```

Ahora que se ha creado el usuario `user3`, asigne a `user3` el rol `collectionFind`.

```
db.grantRolesToUser("user3",["collectionRole"])
```

Por último, tanto `user1` como `user2` abandonan la empresa y su acceso al clúster debe revocarse. Puede hacer esto dejando caer a los usuarios, de la siguiente manera.

```
db.dropUser("user1")
db.dropUser("user2")
```

Para asegurarse de que todos los usuarios tienen los roles adecuados, puede enumerar todos los usuarios con el siguiente comando.

```
show users
```

La salida de esta operación será similar a lo que se indica a continuación.

```
{
   "_id":"serviceadmin",
   "user":"serviceadmin",
   "db":"admin",
   "roles":[
      {
         "db":"admin",
         "role":"root"
      }
   ]
}
{
   "_id":"master-user",
   "user":"master-user",
   "db":"admin",
   "roles":[
      {
         "db":"admin",
         "role":"root"
      }
   ]
}
{
   "_id":"user3",
   "user":"user3",
   "db":"admin",
   "roles":[
      {
         "db":"admin",
```

```
         "role":"collectionRole"
      }
   ]
}
```

Conexión a Amazon DocumentDB como un usuario

Cuando se conecta a un clúster de Amazon DocumentDB, se conecta en el contexto de una base de datos determinada. De forma predeterminada, si no especifica una base de datos en la cadena de conexión, se conectará automáticamente al clúster en el contexto de la base de datos de `test`. Todos los comandos de nivel de recopilación como `insert` y `find` se emiten contra colecciones en la base de datos `test`.

Para ver la base de datos en la que se encuentra o, en otras palabras, en la que está emitiendo comandos, utilice el comando db del intérprete de comandos mongo, de la siguiente manera.

Consulta:

```
db
```

Salida:

```
test
```

Aunque la conexión predeterminada puede estar en el contexto de la base de datos de `test`, eso no significa necesariamente que el usuario asociado a la conexión esté autorizado a realizar acciones en la base de datos de `test`. En el escenario de ejemplo anterior, si se autentica como el usuario `user3`, que tiene el rol `readWrite` de la base de datos `sample-database-1`, el contexto predeterminado de la conexión es la base de datos de `test`. Sin embargo, si intenta insertar un documento en una colección de la base de datos de `test`, recibirá un mensaje de error Authorization failure (Error de autorización). Esto se debe a que ese usuario no está autorizado a realizar ese comando en esa base de datos, como se muestra a continuación.

Consulta:

```
db
```

Salida:

```
test
```

Consulta:

```
db.col.insert({x:1})
```

Salida:

```
WriteCommandError({ "ok" : 0, "code" : 13, "errmsg" : "Authorization failure" })
```

Si cambia el contexto de la conexión a la base de datos `sample-database-1`, puede escribir en la colección para la que el usuario tiene la autorización para hacerlo.

Consulta:

```
use sample-database-1
```

Salida:

```
switched to db sample-database-1
```

Consulta:

```
db.col.insert({x:1})
```

Salida:

```
WriteResult({ "nInserted" : 1})
```

Cuando se autentica en un clúster con un usuario determinado, también puede especificar la base de datos en la cadena de conexión. Al hacerlo, se elimina la necesidad de realizar el comando `use` después de que el usuario haya sido autenticado en la base de datos del `admin`.

La siguiente cadena de conexión autentica al usuario en la base de datos `admin`, pero el contexto de la conexión estará en la base de datos `sample-database-1`.

```
mongo "mongodb://user3:abc123@sample-cluster.node.us-east-1.docdb.amazonaws.com:27017/
sample-database-2"
```

Comandos comunes

Esta sección proporciona ejemplos de comandos comunes que utilizan el control de acceso basado en roles en Amazon DocumentDB. Debe estar en el contexto de la base de datos del `admin` para crear y modificar usuarios y roles. Puede utilizar el comando `use admin` para cambiar a la base de datos del `admin`.

> **Note**
>
> Las modificaciones a los usuarios y roles se producirán implícitamente en la base de datos del `admin`. La creación de usuarios con roles que tienen un ámbito en todas las bases de datos (por ejemplo, `readAnyDatabase`) requiere que esté en el contexto de la base de datos del `admin` (es decir, `use admin`) al crear el usuario, o que indique explícitamente la base de datos para el rol al crear el usuario (como se muestra en el Ejemplo 2 en este).

Ejemplo 1: crear un usuario con el rol `read` para la base de datos `foo`.

```
db.createUser({user: "readInFooBar", pwd: "abc123", roles: [{role: "read", db:
 "foo"}]})
```

La salida de esta operación será similar a lo que se indica a continuación.

```
{
   "user":"readInFooBar",
   "roles":[
      {
         "role":"read",
         "db":"foo"
      }
   ]
}
```

Ejemplo 2: crear un usuario con acceso de lectura en todas las bases de datos.

```
db.createUser({user: "readAllDBs", pwd: "abc123", roles: [{role: "readAnyDatabase", db:
 "admin"}]})
```

La salida de esta operación será similar a lo que se indica a continuación.

```
{
   "user":"readAllDBs",
   "roles":[
      {
         "role":"readAnyDatabase",
         "db":"admin"
      }
   ]
}
```

Ejemplo 3: otorgar el rol `read` a un usuario existente en una nueva base de datos.

```
db.grantRolesToUser("readInFooBar", [{role: "read", db: "bar"}])
```

Ejemplo 4: actualizar el rol de un usuario.

```
db.updateUser("readInFooBar", {roles: [{role: "read", db: "foo"}, {role: "read", db:
 "baz"}]})
```

Ejemplo 5: revocar el acceso a una base de datos de un usuario.

```
db.revokeRolesFromUser("readInFooBar", [{role: "read", db: "baz"}])
```

Ejemplo 6: describir un rol integrado.

```
db.getRole("read", {showPrivileges:true})
```

La salida de esta operación será similar a lo que se indica a continuación.

```
{
   "role":"read",
   "db":"sample-database-1",
   "isBuiltin":true,
   "roles":[

   ],
   "inheritedRoles":[

   ],
   "privileges":[
      {
```

```
         "resource":{
            "db":"sample-database-1",
            "collection":""
         },
         "actions":[
            "changeStream",
            "collStats",
            "dbStats",
            "find",
            "killCursors",
            "listCollections",
            "listIndexes"
         ]
      }
   ],
   "inheritedPrivileges":[
      {
         "resource":{
            "db":"sample-database-1",
            "collection":""
         },
         "actions":[
            "changeStream",
            "collStats",
            "dbStats",
            "find",
            "killCursors",
            "listCollections",
            "listIndexes"
         ]
      }
   }
```

Ejemplo 7: eliminar un usuario del clúster.

```
db.dropUser("readInFooBar")
```

La salida de esta operación será similar a lo que se indica a continuación.

```
true
```

Ejemplo 8: crear un rol con acceso de lectura y escritura a una colección específica

```
db.createRole(
{
    role: "collectionRole",
    privileges: [
    {
        resource: {db: "sample-database-2", collection: "col2"}, actions: ["find",
 "update", "insert", "remove"]
    }],
    roles: []
}
)
```

La salida de esta operación será similar a lo que se indica a continuación.

```
{
   "role":"collectionRole",
   "privileges":[
      {
         "resource":{
            "db":"sample-database-2",
            "collection":"col2"
         },
         "actions":[
            "find",
            "update",
            "insert",
            "remove"
         ]
      }
   ],
   "roles":[

   ]
}
```

Ejemplo 9: crear un usuario y asignar un rol definido por el usuario

```
db.createUser(
{
    user: "user3",
    pwd: "abc123",
    roles: []
```

```
})

db.grantRolesToUser("user3",["collectionRole"])
```

Ejemplo 10: otorgar privilegios adicionales a un rol definido por el usuario

```
db.grantPrivilegesToRole(
  "collectionRole",
  [
    {
      resource: { db: "sample-database-1", collection: "col1" },
      actions: ["find", "update", "insert", "remove"]
    }
  ]
)
```

Ejemplo 11: eliminar privilegios de un rol definido por el usuario

```
db.revokePrivilegesFromRole(
  "collectionRole",
  [
    {
      resource: { db: "sample-database-1", collection: "col2" },
      actions: ["find", "update", "insert", "remove"]
    }
  ]
)
```

Ejemplo 12: actualizar un rol definido por el usuario existente

```
db.updateRole(
  "collectionRole",
  {
    privileges: [
    {
        resource: {db: "sample-database-3", collection: "sample-collection-3"},
 actions: ["find", "update", "insert", "remove"]
    }],
    roles: []
  }
)
```

Diferencias funcionales

En Amazon DocumentDB, las definiciones de usuario y rol se almacenan en la base de datos del `admin` y los usuarios se autentican en la base de datos del `admin`. Esta funcionalidad difiere de la MongoDB Community Edition, pero es consistente con MongoDB Atlas.

Amazon DocumentDB también admite flujos de cambios, lo que brinda una secuencia en orden cronológico de los eventos de actualización que se producen dentro de las colecciones de su clúster. La acción `listChangeStreams` se aplica en el nivel de clúster (es decir, en todas las bases de datos) y la acción `modifyChangeStreams` puede aplicarse en el nivel de base de datos y en el nivel de clúster.

Límites de las s

La siguiente tabla contiene los límites del control de acceso basado en roles en Amazon DocumentDB.

Description (Descripción)	Límite
Número de usuarios por clúster	1 000
Número de roles asociados a un usuario	1 000
Número de roles definidos por el usuario	100
Número de recursos asociados a un privilegio	100

Acceso a la base de datos mediante el control de acceso basado en roles

Con el control de acceso basado en roles, puede crear un usuario y otorgarle uno o más roles para determinar qué operaciones puede realizar el usuario en una base de datos o clúster.

A continuación se muestra una lista de roles integrados que se admiten actualmente en Amazon DocumentDB.

> **Note**
>
> En Amazon DocumentDB 4.0 y 5.0, los comandos `ListCollection` y `ListDatabase` pueden usar, de forma opcional, los parámetros `authorizedCollections` y

`authorizedDatabases` para enumerar las colecciones y bases de datos a las que el usuario tiene permiso para acceder, con los roles `listCollections` y `listDatabase`, respectivamente. Ahora, los usuarios pueden eliminar sus propios cursores sin necesitar el rol `KillCursor`.

Database user

Nombre del rol	Description (Descripción)	Acciones

`read`	Otorga a un usuario acceso de lectura a la base de datos especificada.	`changeStreams`
		`collStats`
		`dbStats`
		`find`
		`killCursors`
		`listIndexes`
		`listCollections`

`readWrite`	Otorga al usuario acceso de lectura y escritura a la base de datos especificada.	Todas las acciones de los permisos `read`.
		`createCollection`
		`dropCollection`
		`createIndex`
		`dropIndex`
		`insert`
		`killCursors`

Nombre del rol	Description (Descripción)	Acciones

		`listIndexes`
		
		`listColle ctions`
		
		`remove`
		
		`update`

Cluster user

Nombre del rol	Description (Descripción)	Acciones

readAnyDatabase	Otorga a un usuario acceso de lectura a todas las bases de datos del clúster.	Todas las acciones de los permisos `read`.
		
		`listChang eStreams`
		
		`listDatabases`

`readWrite AnyDatabase`	Otorga a un usuario accesos de lectura y escritura a todas las bases de datos del clúster.	Todas las acciones de los permisos `readWrite` .
		
		`listChang eStreams`
		
		`listDatabases`

`userAdmin AnyDatabase`	Otorga al usuario la capacidad de asignar y modificar los roles o privilegios que cualquier usuario tiene en la base de datos especific ada.	`changeCus tomData`
		
		`changePassword`
		
		`createUser`

Nombre del rol	Description (Descripción)	Acciones

		`dropRole`
		`dropUser`
		`grantRole`
		`listDatabases`
		`revokeRole`
		`viewRole`
		`viewUser`

`dbAdminAnyDatabase`	Otorga al usuario la capacidad de realizar funciones de administración de bases de datos en cualquier base de datos especificada.	Todas las acciones de los permisos `dbAdmin`.
		`dropCollection`
		`listDatabases`
		`listChangeStreams`
		`modifyChangeStreams`

Superuser

Nombre del rol	Description (Descripción)	Acciones
`root`	Otorga a un usuario acceso a los recursos y operaciones de todos los siguientes roles combinados: `readWriteAnyDatabase`, `dbAdminAnyDatabase`, `userAdminAnyDatabase`, `clusterAdmin`, `restore`, y `backup`.	Todas las acciones de `readWriteAnyDatabase`, `dbAdminAnyDatabase`, `dbAdminAnyDatabase`

Nombre del rol	Description (Descripción)	Acciones
		, `userAdmin` `AnyDatabase` , `clusterAdmin` , `restore`, y `backup`.

Database administrator

Nombre del rol	Description (Descripción)	Acciones

`dbAdmin`	Otorga al usuario la capacidad de realizar tareas administrativas en la base de datos especificada.	`bypassDocumentValidation`
		`collMod`
		`collStats`
		`createCollection`
		`createIndex`
		`dropCollection`
		`dropDatabase`
		`dropIndex`
		`dbStats`
		`find`
		`killCursors`
		`listIndexes`
		`listCollections`

Nombre del rol	Description (Descripción)	Acciones
		`modifyChangeStreams`
`dbOwner`	Otorga al usuario la capacidad de realizar cualquier tarea administrativa en la base de datos especificada combinando los roles `dbAdmin` y `readWrite` .	Todas las acciones de `dbAdmin` y `readWrite` .

Cluster administrator

Role name (Nombre de rol)	Description (Descripción)	Acciones

`clusterAdmin`	Otorga a un usuario el mayor acceso a la administración de clústeres mediante la combinación de los roles `clusterManager` , `clusterMonitor` y `hostManager` .	Todas las acciones de `clusterManager` , `clusterMonitor` y `hostManager` .
		
		`listChangeStreams`
		
		`dropDatabase`
		
		`modifyChangeStreams`

`clusterManager`	Otorga al usuario la capacidad de realizar acciones de administración y supervisión en el clúster especificado.	`listChangeStreams`
		
		`listSessions`
		
		`modifyChangeStreams`

Role name (Nombre de rol)	Description (Descripción)	Acciones
		`replSetGetConfig`

`clusterMonitor`	Otorga a un usuario la capacidad de tener acceso de solo lectura a las herramientas de supervisión.	`collStats`
		`dbStats`
		`find`
		`getParameter`
		`hostInfo`
		`indexStats`
		`killCursors`
		`listChangeStreams`
		`listCollections`
		`listDatabases`
		`listIndexes`
		`listSessions`
		`replSetGetConfig`
		`serverStatus`
		`top`

Role name (Nombre de rol)	Description (Descripción)	Acciones

`hostManager`	Otorga al usuario la capacidad de supervisar y administrar servidores.	`auditConfigure`
		`killCursors`
		`killAnyCursor`
		`killAnySession`
		`killop`

Backup administrator

Nombre del rol	Description (Descripción)	Acciones

`backup`	Otorga a un usuario el acceso necesario para realizar copias de seguridad de los datos.	`getParameter`
		`insert`
		`find`
		`listChangeStreams`
		`listCollections`
		`listDatabases`
		`listIndexes`
		`update`

`restore`	Otorga a un usuario el acceso necesario para restaurar los datos.	`bypassDocumentValidation`

Nombre del rol	Description (Descripción)	Acciones
		changeCustomData changePassword collMod createCollection createIndex createUser dropCollection dropRole dropUser getParameter grantRole find insert listCollections modifyChangeStreams revokeRole remove viewRole viewUser

Nombre del rol	Description (Descripción)	Acciones
		`update`

Registro y supervisión en Amazon DocumentDB

Amazon DocumentDB (con compatibilidad con MongoDB) proporciona diversas métricas de Amazon CloudWatch que se pueden monitorizar para determinar el estado y el rendimiento de los clústeres e instancias de Amazon DocumentDB. Puede ver las métricas de Amazon DocumentDB mediante diversas herramientas, como la consola Amazon DocumentDB, la AWS CLI, la consola de Amazon CloudWatch y CloudWatch API. Para obtener más información sobre la supervisión, consulte Monitorización de Amazon DocumentDB.

Además de las métricas de Amazon CloudWatch, puede utilizar el generador de perfiles para registrar el tiempo de ejecución y los detalles de las operaciones realizadas en el clúster. El generador de perfiles es útil para monitorizar las operaciones más lentas del clúster para ayudarle a mejorar el rendimiento de las consultas individuales y el rendimiento general del clúster. Cuando se habilita, las operaciones se registran en los registros de Amazon CloudWatch y se puede utilizar CloudWatch Insight para analizar, monitorizar y archivar los datos de creación de perfiles de Amazon DocumentDB. Para obtener más información, consulte Creación de perfiles de operaciones en Amazon DocumentDB.

Amazon DocumentDB también se integra con CloudTrail de AWS, un servicio que proporciona un registro de las medidas adoptadas por usuarios, roles o un servicio de AWS en Amazon DocumentDB (compatible con MongoDB). CloudTrail obtiene todas las llamadas a la API de la AWS CLI para Amazon DocumentDB como eventos, incluidas las llamadas procedentes de la Consola de administración de AWS de Amazon DocumentDB y las llamadas de código a las operaciones de la SDK de Amazon DocumentDB. Para obtener más información, consulte Registro de llamadas a la API de Amazon DocumentDB con AWS CloudTrail.

Con Amazon DocumentDB puede auditar los eventos que se han realizado en su clúster. Los intentos de autenticación correctos e incorrectos, la eliminación de una colección en una base de datos o la creación de un índice son algunos ejemplos de eventos registrados. De forma predeterminada, la auditoría está deshabilitada en Amazon DocumentDB y, para utilizar esta característica, es necesario suscribirse. Para obtener más información, consulte Auditoría de eventos de Amazon DocumentDB.

Actualización de los certificados TLS de Amazon DocumentDB

Temas

- Actualización de la aplicación y del clúster de Amazon DocumentDB
- Rotación automática de certificados del servidor
- Solución de problemas
- Preguntas frecuentes

El certificado de la autoridad de certificación (CA) para los clústeres de Amazon DocumentDB se actualizó en agosto de 2024. Si utiliza clústeres de Amazon DocumentDB con Seguridad de la capa de transporte (TLS) habilitada (la configuración predeterminada) y no ha rotado los certificados de servidor y aplicación cliente, se requieren los pasos siguientes para mitigar los problemas de conectividad entre la aplicación y los clústeres de Amazon DocumentDB.

- Paso 1: Descargar el nuevo certificado de CA y actualizar la aplicación
- Paso 2: Actualizar el certificado de servidor

Los certificados de CA y del servidor se actualizaron de conformidad con las prácticas recomendadas de mantenimiento y seguridad estándar para Amazon DocumentDB. Las aplicaciones cliente deben añadir los nuevos certificados de CA a sus almacenes de confianza y las instancias de Amazon DocumentDB existentes deben actualizarse para utilizar los nuevos certificados de CA antes de esta fecha de vencimiento.

Actualización de la aplicación y del clúster de Amazon DocumentDB

Siga los pasos indicados en esta sección para actualizar el grupo de certificados de CA de la aplicación (Paso 1) y los certificados de servidor del clúster (Paso 2). Antes de aplicar los cambios a los entornos de producción, recomendamos encarecidamente probar estos pasos en un entorno de desarrollo o ensayo.

> **Note**
>
> Debe completar los pasos 1 y 2 en cada Región de AWS en la que tenga clústeres de Amazon DocumentDB.

Paso 1: Descargar el nuevo certificado de CA y actualizar la aplicación

Descargue el nuevo certificado de CA y actualice su aplicación de tal forma que use este nuevo certificado de CA para crear las conexiones TLS a Amazon DocumentDB. Descargue el nuevo paquete de certificados de CA desde https://truststore.pki.rds.amazonaws.com/global/global-bundle.pem. Esta operación descarga un archivo llamado `global-bundle.pem`.

> **Note**
>
> Si accede al almacén de claves que incluye tanto el certificado de CA antiguo (`rds-ca-2019-root.pem`) como los nuevos (`rds-ca-rsa2048-g1`, `rds-ca-rsa4096-g1`, `rds-ca-ecc384-g1`) compruebe que el almacén de claves tenga seleccionado `global-bundle`.

```
wget https://truststore.pki.rds.amazonaws.com/global/global-bundle.pem
```

A continuación, actualice las aplicaciones de tal forma que utilicen el nuevo paquete de certificados. El nuevo paquete de CA contiene tanto el certificado de CA anterior (rds-ca-2019) como los certificados de CA nuevos (rds-ca-rsa2048-g1, rds-ca-rsa4096-g1, rds-ca-ecc384-g1). Al tener ambos certificados de CA en el nuevo paquete de CA puede actualizar la aplicación y el clúster en dos pasos.

Para las aplicaciones de Java, se debe crear un nuevo almacén de confianza con el nuevo certificado de CA. Para obtener instrucciones, consulte la pestaña de Java del tema Conexión con TLS habilitado.

Para comprobar que la aplicación utiliza el último grupo de certificados de CA, consulte ¿Cómo puedo estar seguro de que estoy usando el paquete de CA más reciente?. Si ya está utilizando el último grupo de certificados de CA en la aplicación, puede saltar al paso 2.

Para obtener ejemplos de uso de un grupo de CA con su aplicación, consulte Cifrado de datos en tránsito y Conexión con TLS habilitado.

> **Note**
>
> Actualmente, MongoDB Go Driver 1.2.1 sólo acepta un certificado de servidor de CA en `sslcertificateauthorityfile`. Consulte Conexión con TLS habilitado para conectarse a Amazon DocumentDB mediante Go cuando TLS esté habilitado.

Paso 2: Actualizar el certificado de servidor

Después de que la aplicación se haya actualizado con el fin de utilizar el nuevo paquete de CA, el siguiente paso consiste en actualizar el certificado de servidor al modificar cada instancia en un clúster de Amazon DocumentDB. Para modificar instancias para utilizar el nuevo certificado de servidor, consulte las instrucciones siguientes.

Amazon DocumentDB proporciona las siguientes CA para firmar el certificado del servidor de base de datos de una instancia de base de datos:

- rds-ca-ecc384-g1: utiliza una entidad de certificación con el algoritmo de clave privada RSA 384 y el algoritmo de firma SHA384. Esta CA admite la rotación automática de certificados de servidor. Solo es compatible con Amazon DocumentDB 4.0 y 5.0.
- rds-ca-rsa2048-g1: utiliza una entidad de certificación con el algoritmo de clave privada RSA 2048 y el algoritmo de firma SHA256 en la mayoría de las regiones de AWS. Esta CA admite la rotación automática de certificados de servidor.
- rds-ca-rsa4096-g1: utiliza una entidad de certificación con el algoritmo de clave privada RSA 4096 y el algoritmo de firma SHA384. Esta CA admite la rotación automática de certificados de servidor.

> **Note**
>
> Si utiliza la AWS CLI, puede ver la validez de las entidades de certificación enumeradas anteriormente mediante describe-certificates.

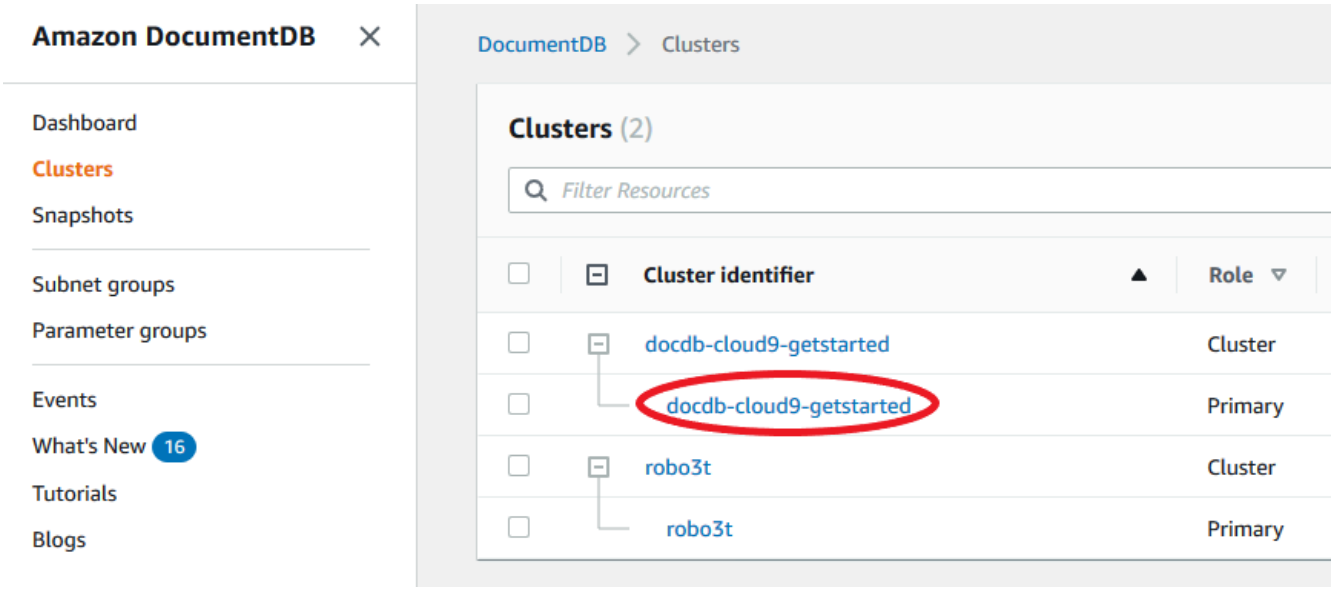
Estos certificados de CA se incluyen en el paquete de certificados regionales y globales. Al utilizar la CA rds-ca-rsa2048-g1, rds-ca-rsa4096-g1 o rds-ca-ecc384-g1 con una base de datos, Amazon DocumentDB administra el certificado del servidor de base de datos en la base de datos. Amazon DocumentDB rota el certificado del servidor de base de datos de forma automática antes de que caduque.

> **Note**
>
> Amazon DocumentDB no requiere un reinicio para la rotación de certificados si el clúster se ejecuta en las siguientes versiones de parches del motor:
>
> - Amazon DocumentDB 3.6: 1.0.208662 o posterior
> - Amazon DocumentDB 4.0: 2.0.10179 o posterior
> - Amazon DocumentDB 5.0: 3.0.4780 o posterior
>
> Para determinar la versión de parche actual del motor de Amazon DocumentDB, ejecute el siguiente comando: `db.runCommand({getEngineVersion: 1})`.
> Antes de actualizar el certificado de servidor, asegúrese de haber completado Paso 1.

Using the Consola de administración de AWS

Complete los pasos siguientes para identificar y rotar el certificado de servidor antiguo para las instancias de Amazon DocumentDB existentes mediante la Consola de administración de AWS.

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon DocumentDB en https://console.aws.amazon.com/docdb.
2. En la lista de regiones en la esquina superior derecha de la pantalla, seleccione la Región de AWS en la que residen sus clústeres.
3. En el panel de navegación en el lado izquierdo de la consola, en DAX, elija Clústeres.
4. Es posible que necesite identificar qué instancias siguen en el antiguo certificado de servidor (`rds-ca-2019`). Puede hacerlo en la columna Autoridad de certificación, que se encuentra en el extremo derecho de la tabla Clústeres.
5. En la tabla Clústeres, verá la columna Identificador del clúster en el extremo izquierdo. Las instancias se muestran en clústeres, de forma similar a la siguiente captura de pantalla.



6. Marque la casilla de verificación situada a la izquierda de la instancia de su interés.
7. Elija Actions (Acciones) y después Modify (Modificar).
8. En Certificate authority (Entidad de certificación), seleccione el nuevo certificado de servidor (`rds-ca-rsa2048-g1`) para esta instancia.
9. Puede ver un resumen de los cambios en la página siguiente. Tenga en cuenta que se muestra una alerta adicional para recordarle que debe asegurarse de que su aplicación utilice el paquete más reciente de certificados de CA antes de modificar la instancia, con el fin de evitar que se interrumpa la conectividad.
10. Puede optar por aplicar la modificación durante el próximo periodo de mantenimiento o bien aplicarla de inmediato. Si su intención es modificar el certificado del servidor inmediatamente, utilice la opción Apply immediately (Aplicar inmediatamente).
11. Seleccione Modify instance (Modificar instancia) para completar la actualización.

Using the AWS CLI

Complete los pasos siguientes para identificar y rotar el certificado de servidor antiguo para las instancias de Amazon DocumentDB existentes mediante la AWS CLI.

1. Para modificar las instancias de inmediato, ejecute el siguiente comando para cada instancia del clúster.

```
aws docdb modify-db-instance --db-instance-identifier <yourInstanceIdentifier>
 --ca-certificate-identifier rds-ca-rsa2048-g1 --apply-immediately
```

2. Para modificar las instancias de los clústeres de tal forma que usen el nuevo certificado de CA durante el próximo periodo de mantenimiento del clúster, ejecute el siguiente comando para cada instancia del clúster.

```
aws docdb modify-db-instance --db-instance-identifier <yourInstanceIdentifier>
 --ca-certificate-identifier rds-ca-rsa2048-g1 --no-apply-immediately
```

Rotación automática de certificados del servidor

Amazon DocumentDB admite la rotación automática de certificados del servidor. El certificado del servidor es el certificado de entidad final emitido para cada instancia del clúster. A diferencia de los certificados CA raíz, los certificados del servidor tienen una validez corta (12 meses) y Amazon DocumentDB gestiona su rotación automáticamente sin que usted tenga que realizar ninguna acción. Amazon DocumentDB utiliza la misma CA raíz para esta rotación automática, por lo que no es necesario descargar un nuevo paquete de CA.

> **Important**
>
> Cuando se conecte al clúster de Amazon DocumentDB, le recomendamos que confíe en el paquete de CA raíz en lugar de confiar directamente en cada certificado del servidor. Esto evitará errores de conexión después de rotar el certificado del servidor. Consulte Conexión con TLS habilitado.

Amazon DocumentDB intenta rotar el certificado del servidor durante el período de mantenimiento que prefiera a la mitad de la vida del certificado del servidor. El nuevo certificado del servidor es válido durante 12 meses.

Utilice el comando `describe-db-engine-versions` e inspeccione el indicador `SupportsCertificateRotationWithoutRestart` para identificar si la versión del motor admite la rotación del certificado sin reinicio.

> **Note**
>
> Amazon DocumentDB admite la rotación de certificados del servidor sin reinicio si el clúster se ejecuta en las siguientes versiones de parches del motor:
>
> - Amazon DocumentDB 3.6: 1.0.208662 o posterior

- Amazon DocumentDB 4.0: 2.0.10179 o posterior
- Amazon DocumentDB 5.0: 3.0.4780 o posterior

Para determinar la versión del parche actual del motor de Amazon DocumentDB, ejecute este comando: `db.runCommand({getEngineVersion: 1})`.
Si utiliza una versión anterior del parche del motor, Amazon DocumentDB rotará el certificado del servidor y programará un evento de reinicio de la base de datos en el período de mantenimiento que prefiera.

Solución de problemas

Si tiene problemas para conectarse al clúster como parte de la rotación de certificados, le sugerimos lo siguiente:

- Compruebe que sus clientes están utilizando el paquete de certificados más reciente. Consulte ¿Cómo puedo estar seguro de que estoy usando el paquete de CA más reciente?.
- Compruebe que las instancias están utilizando el certificado más reciente. Consulte ¿Cómo puedo saber cuáles de mis instancias de Amazon DocumentDB usan el certificado de servidor antiguo/nuevo?.
- Compruebe que la última entidad emisora de certificados está siendo utilizada por la aplicación. Algunos controladores, como Java y Go, requieren código adicional para importar varios certificados de un paquete de certificados al almacén de confianza. Para obtener más información sobre cómo conectarse a Amazon DocumentDB con TLS, consulte Conexión mediante programación a Amazon DocumentDB.
- Póngase en contacto con el soporte. Si tiene preguntas o problemas, póngase en contacto con Soporte.

Preguntas frecuentes

A continuación se presentan respuestas a algunas preguntas comunes acerca de los certificados TLS.

¿Qué hago si tengo preguntas o problemas?

Si tiene preguntas o problemas, póngase en contacto con Soporte.

¿Cómo sé si estoy usando TLS para conectarme a mi clúster de Amazon DocumentDB?

Para determinar si el clúster usa TLS, examine el parámetro `tls` del grupo de parámetros del clúster. Si el parámetro `tls` se encuentra establecido en `enabled`, está utilizando el certificado TLS para conectarse al clúster. Para obtener más información, consulte Administración de los grupos de parámetros de clúster de Amazon DocumentDB.

¿Por qué hay que actualizar los certificados de CA y de servidor?

Los certificados de CA y de servidor de Amazon DocumentDB se están actualizando de conformidad con las prácticas recomendadas de mantenimiento y seguridad estándar para Amazon DocumentDB.

¿Qué sucede si no realizo ninguna acción antes de la fecha de caducidad?

Si utiliza TLS para conectarse al clúster de Amazon DocumentDB con un certificado CA vencido, las aplicaciones que se conectan a través de TLS ya no podrán comunicarse más con el clúster de Amazon DocumentDB.

Amazon DocumentDB no rotará los certificados de la base de datos automáticamente antes de la fecha de caducidad. Debe actualizar las aplicaciones y los clústeres para utilizar los nuevos certificados de CA antes o después de la fecha de caducidad.

¿Cómo puedo saber cuáles de mis instancias de Amazon DocumentDB usan el certificado de servidor antiguo/nuevo?

Para identificar las instancias de Amazon DocumentDB que siguen utilizando el certificado de servidor antiguo, puede utilizar la Consola de administración de AWS o la AWS CLI de Amazon DocumentDB.

Uso de Consola de administración de AWS

Identificación de las instancias de los clústeres que utilizan el certificado anterior

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon DocumentDB en https://console.aws.amazon.com/docdb.
2. En la lista de regiones de la parte superior derecha de la pantalla, elija la Región de AWS en la que residen sus instancias.
3. En el panel de navegación en el lado izquierdo de la consola, en DAX, elija Clústeres.

4. En la columna Autoridad de certificación (cerca del extremo derecho de la tabla), se muestran las instancias que todavía contienen el certificado de servidor antiguo (`rds-ca-2019`) y el certificado de servidor nuevo (`rds-ca-rsa2048-g1`).

Uso de AWS CLI

Para identificar las instancias de los clústeres que utilizan el certificado de servidor anterior, utilice el comando `describe-db-clusters` con lo siguiente.

```
aws docdb describe-db-instances \
    --filters Name=engine,Values=docdb \
    --query 'DBInstances[*].
{CertificateVersion:CACertificateIdentifier,InstanceID:DBInstanceIdentifier}'
```

¿Cómo puedo modificar instancias individuales de mi clúster de Amazon DocumentDB para actualizar el certificado de servidor?

Recomendamos actualizar al mismo tiempo los certificados de servidor de todas las instancias de un clúster determinado. Para modificar las instancias del clúster, puede utilizar la consola o la AWS CLI.

> **Note**
>
> Antes de actualizar el certificado de servidor, asegúrese de haber completado el paso 1.

Uso de Consola de administración de AWS

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon DocumentDB en https://console.aws.amazon.com/docdb.
2. En la lista de regiones en la esquina superior derecha de la pantalla, seleccione la Región de AWS en la que residen sus clústeres.
3. En el panel de navegación en el lado izquierdo de la consola, en DAX, elija Clústeres.
4. En la columna Autoridad de certificación (cerca del extremo derecho de la tabla), se muestran las instancias que todavía contienen el certificado de servidor antiguo (`rds-ca-2019`).
5. En la tabla Clústeres, en Identificador del clúster, seleccione una instancia para modificarla.
6. Elija Actions (Acciones) y después Modify (Modificar).

7. En Certificate authority (Entidad de certificación), seleccione el nuevo certificado de servidor (`rds-ca-rsa2048-g1`) para esta instancia.
8. Puede ver un resumen de los cambios en la página siguiente. Tenga en cuenta que se muestra una alerta adicional para recordarle que debe asegurarse de que su aplicación utilice el paquete más reciente de certificados de CA antes de modificar la instancia, con el fin de evitar que se interrumpa la conectividad.
9. Puede optar por aplicar la modificación durante el próximo periodo de mantenimiento o bien aplicarla de inmediato.
10. Seleccione Modify instance (Modificar instancia) para completar la actualización.

Uso de AWS CLI

Complete los pasos siguientes para identificar y rotar el certificado de servidor antiguo para las instancias de Amazon DocumentDB existentes mediante la AWS CLI.

1. Para modificar las instancias de inmediato, ejecute el siguiente comando para cada instancia del clúster.

```
aws docdb modify-db-instance --db-instance-identifier <yourInstanceIdentifier> --
ca-certificate-identifier rds-ca-rsa2048-g1 --apply-immediately
```

2. Para modificar las instancias de los clústeres de tal forma que usen el nuevo certificado de CA durante el próximo periodo de mantenimiento del clúster, ejecute el siguiente comando para cada instancia del clúster.

```
aws docdb modify-db-instance --db-instance-identifier <yourInstanceIdentifier> --
ca-certificate-identifier rds-ca-rsa2048-g1 --no-apply-immediately
```

¿Qué sucede si añado una nueva instancia a un clúster existente?

Todas las instancias nuevas que se creen utilizan el certificado de servidor antiguo y requieren conexiones TLS que usen el certificado de CA antiguo. Cualquier instancia nueva de Amazon DocumentDB creada después del 25 de enero de 2024 utilizará de forma predeterminada el nuevo certificado rds-ca-rsa2048-g1.

¿Qué sucede si se sustituye una instancia o se produce una conmutación por error en el clúster?

Si se sustituye una instancia en el clúster, la nueva instancia que se crea continúa usando el mismo certificado de servidor que se estaba utilizando anteriormente. Se recomienda actualizar los certificados de servidor para todas las instancias al mismo tiempo. Si se produce una conmutación por error en el clúster, se usará el certificado de servidor del nuevo nodo principal.

Si no uso TLS para conectarme al clúster, ¿tengo que actualizar todas las instancias?

Recomendamos encarecidamente habilitar TLS. En caso de que no habilite TLS, le recomendamos que rote los certificados de las instancias de Amazon DocumentDB si planea usar TLS para conectarse a los clústeres en el futuro. Si no planea usar nunca TLS para conectarse a los clústeres de Amazon DocumentDB, no es necesaria ninguna acción.

Si no estoy usando TLS para conectarme a mi clúster pero tengo previsto hacerlo en el futuro, ¿qué tengo que hacer?

Si creó un clúster antes de enero de 2024, siga el paso 1 y el paso 2 de la sección anterior para asegurarse de que la aplicación utiliza la agrupación de CA actualizada y de que cada instancia de Amazon DocumentDB utiliza el certificado de servidor más reciente. Si crea un clúster después del 25 de enero de 2024, el clúster ya tendrá el certificado de servidor más reciente (rds-ca-rsa2048-g1). Para comprobar que la aplicación utiliza el grupo de CA más reciente, consulte Si no uso TLS para conectarme al clúster, ¿tengo que actualizar todas las instancias?

¿Puede prorrogarse el plazo más allá de agosto de 2024?

Si sus aplicaciones se conectan a través de TLS, la fecha límite no se podrá prorrogar.

¿Cómo puedo estar seguro de que estoy usando el paquete de CA más reciente?

Para comprobar que tiene el paquete más reciente, use el siguiente comando. Para ejecutar este comando, debe tener Java instalado y las herramientas de Java deben estar en la variable PATH de su shell. Para obtener más información, consulte Uso de Java.

macOS y Amazon Linux

```
keytool -printcert -v -file global-bundle.pem
```

Windows

```
keytool -printcert -v -file global-bundle.p7b
```

¿Por qué veo “RDS” en el nombre del paquete de CA?

Para determinadas funciones de administración, como la administración de certificados, Amazon DocumentDB utiliza tecnología operativa que se comparte con Amazon Relational Database Service (Amazon RDS).

¿Cuándo caduca el nuevo certificado?

El nuevo certificado del servidor caducará (por lo general) de la siguiente manera:

- rds-ca-rsa2048-g1: caduca en 2061
- rds-ca-rsa4096-g1: caduca en 2121
- rds-ca-ecc384-g1: caduca en 2121

¿Qué tipo de errores veré si no tomo medidas antes de que caduque el certificado?

Los mensajes de error variarán en función del controlador. En general, verá errores de validación de certificados que contienen la cadena “el certificado ha caducado”.

Si he aplicado el nuevo certificado de servidor, ¿puedo revertirlo al certificado de servidor antiguo?

Si necesita revertir una instancia al certificado de servidor antiguo, recomendamos que haga lo mismo para todas las instancias del clúster. Puede revertir el certificado de servidor para cada instancia de un clúster mediante la Consola de administración de AWS o la AWS CLI.

Uso de Consola de administración de AWS

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon DocumentDB en https://console.aws.amazon.com/docdb.
2. En la lista de regiones en la esquina superior derecha de la pantalla, seleccione la Región de AWS en la que residen sus clústeres.
3. En el panel de navegación en el lado izquierdo de la consola, en DAX, elija Clústeres.

4. En la tabla Clústeres, en Identificador del clúster, seleccione una instancia para modificarla. Elija Actions (Acciones) y después Modify (Modificar).
5. En Certificate authority (Entidad de certificación), puede seleccionar el certificado de servidor antiguo (`rds-ca-2019`).
6. Elija Continue (Continuar) para ver un resumen de las modificaciones.
7. En la página que aparece, puede elegir programar las modificaciones para que se apliquen en el próximo periodo de mantenimiento o aplicar las modificaciones inmediatamente. Realice la selección y elija Modify instance (Modificar instancia).

> **Note**
>
> Si opta por aplicar las modificaciones inmediatamente, también se aplican los cambios de la cola de modificaciones pendientes. Si alguna de las modificaciones pendientes requiere un tiempo de inactividad, elegir esta opción puede provocar un tiempo de inactividad inesperado.

Uso de AWS CLI

```
aws docdb modify-db-instance --db-instance-identifier <db_instance_name> ca-
certificate-identifier rds-ca-2019 <--apply-immediately | --no-apply-immediately>
```

Si elige `--no-apply-immediately`, los cambios se aplicarán durante el próximo periodo de mantenimiento del clúster.

Si restauro a partir de una instantánea o de una restauración puntual, ¿tendrá el nuevo certificado de servidor?

Si restaura una instantánea o realiza una restauración puntual después de agosto de 2024, el nuevo clúster que se crea utilizará el nuevo certificado de entidad de certificación.

¿Qué sucede si tengo problemas para conectarme directamente a mi clúster de Amazon DocumentDB desde cualquier versión de Mac OS?

Mac OS ha actualizado los requisitos para certificados de confianza. Ahora los certificados de confianza deben tener una validez de 397 días o menos (consulte https://support.apple.com/en-us/HT211025).

> **Note**
>
> Esta restricción se observa en las versiones más recientes de Mac OS.

Los certificados de instancia de Amazon DocumentDB son válidos durante más de cuatro años, más que el máximo de Mac OS. Para conectarse directamente a un clúster de Amazon DocumentDB desde un equipo que ejecuta Mac OS, debe permitir certificados no válidos al crear la conexión TLS. En este caso, los certificados no válidos significan que el período de validez es superior a 397 días. Debe comprender los riesgos antes de permitir certificados no válidos al conectarse al clúster de Amazon DocumentDB.

Para conectarse a un clúster de Amazon DocumentDB desde Mac OS utilizando la AWS CLI, utilice el parámetro `tlsAllowInvalidCertificates`.

```
mongo --tls --host <hostname> --username <username> --password <password> --port 27017
 --tlsAllowInvalidCertificates
```

Actualización de los certificados TLS de Amazon DocumentDB: GovCloud

Temas

- Actualización de la aplicación y del clúster de Amazon DocumentDB
- Solución de problemas
- Preguntas frecuentes

> **Note**
>
> Esta información solo se aplica a usuarios de las regiones de GovCloud (Este de EE. UU.) y GovCloud (Oeste de EE. UU.).

El certificado de la autoridad de certificación (CA) para los clústeres de Amazon DocumentDB (con compatibilidad con MongoDB) se actualizará el 18 de mayo de 2022. Si utiliza clústeres de Amazon DocumentDB con Seguridad de la capa de transporte (TLS) habilitada (la configuración

predeterminada) y no ha rotado los certificados de servidor y aplicación cliente, se requieren los pasos siguientes para mitigar los problemas de conectividad entre la aplicación y los clústeres de Amazon DocumentDB.

- Paso 1: Descargar el nuevo certificado de CA y actualizar la aplicación
- Paso 2: Actualizar el certificado de servidor

Los certificados de CA y del servidor se actualizaron de conformidad con las prácticas recomendadas de mantenimiento y seguridad estándar para Amazon DocumentDB. El certificado de CA anterior caducará el 18 de mayo de 2022. Las aplicaciones cliente deben añadir los nuevos certificados de CA a sus almacenes de confianza y las instancias de Amazon DocumentDB existentes deben actualizarse para utilizar los nuevos certificados de CA antes de esta fecha de vencimiento.

Actualización de la aplicación y del clúster de Amazon DocumentDB

Siga los pasos indicados en esta sección para actualizar el grupo de certificados de CA de la aplicación (Paso 1) y los certificados de servidor del clúster (Paso 2). Antes de aplicar los cambios a los entornos de producción, recomendamos encarecidamente probar estos pasos en un entorno de desarrollo o ensayo.

> **Note**
>
> Debe completar los pasos 1 y 2 en cada Región de AWS en la que tenga clústeres de Amazon DocumentDB.

Paso 1: Descargar el nuevo certificado de CA y actualizar la aplicación

Descargue el nuevo certificado de CA y actualice la aplicación de tal forma que use este nuevo certificado de CA para crear las conexiones TLS a Amazon DocumentDB en su región específica:

- Para GovCloud (Oeste de EE. UU.), descargue el nuevo paquete de certificados de CA de https://truststore.pki.us-gov-west-1.rds.amazonaws.com/us-gov-west-1/us-gov-west-1-bundle.pem. Esta operación descarga un archivo llamado `us-gov-west-1-bundle.pem`.
- Para GovCloud (Este de EE. UU.), descargue el nuevo paquete de certificados de CA de https://truststore.pki.us-gov-west-1.rds.amazonaws.com/us-gov-east-1/us-gov-east-1-bundle.pem. Esta operación descarga un archivo llamado `us-gov-east-1-bundle.pem`.

> **Note**
>
> Si accede al almacén de claves que incluye tanto el certificado de CA antiguo (`rds-ca-2017-root.pem`) como los nuevos (`rds-ca-rsa2048-g1.pem`, `rds-ca-rsa4096-g1.pem` o `rds-ca-ecc384-g1.pem`), compruebe que el almacén de claves tenga seleccionado el certificado elegido. Para obtener más información sobre cada certificado, consulte el paso 2 que aparece a continuación.

```
wget https://truststore.pki.us-gov-west-1.rds.amazonaws.com/us-gov-west-1/us-gov-west-1-bundle.pem
```

```
wget https://truststore.pki.us-gov-west-1.rds.amazonaws.com/us-gov-east-1/us-gov-east-1-bundle.pem
```

A continuación, actualice las aplicaciones de tal forma que utilicen el nuevo paquete de certificados. La nueva agrupación de CA contiene tanto el certificado de CA antiguo como el nuevo (`rds-ca-rsa2048-g1.pem`, `rds-ca-rsa4096-g1.pem` o `rds-ca-ecc384-g1.pem`). Al tener ambos certificados de CA en el nuevo paquete de CA puede actualizar la aplicación y el clúster en dos pasos.

En todas las descargas de la agrupación de certificados de CA posteriores al 21 de diciembre de 2021, se deberá utilizar la nueva agrupación de certificados de CA. Para comprobar que la aplicación utiliza el último grupo de certificados de CA, consulte ¿Cómo puedo estar seguro de que estoy usando el paquete de CA más reciente?. Si ya está utilizando el último grupo de certificados de CA en la aplicación, puede saltar al paso 2.

Para obtener ejemplos de uso de un grupo de CA con su aplicación, consulte Cifrado de datos en tránsito y Conexión con TLS habilitado.

> **Note**
>
> Actualmente, MongoDB Go Driver 1.2.1 sólo acepta un certificado de servidor de CA en `sslcertificateauthorityfile`. Consulte Conexión con TLS habilitado para conectarse a Amazon DocumentDB mediante Go cuando TLS esté habilitado.

Paso 2: Actualizar el certificado de servidor

Después de que la aplicación se haya actualizado con el fin de utilizar el nuevo paquete de CA, el siguiente paso consiste en actualizar el certificado de servidor al modificar cada instancia en un clúster de Amazon DocumentDB. Para modificar instancias para utilizar el nuevo certificado de servidor, consulte las instrucciones siguientes.

Amazon DocumentDB proporciona las siguientes CA para firmar el certificado del servidor de base de datos de una instancia de base de datos:

- rds-ca-ecc384-g1: utiliza una entidad de certificación con el algoritmo de clave privada RSA 384 y el algoritmo de firma SHA384. Esta CA admite la rotación automática de certificados de servidor. Solo es compatible con Amazon DocumentDB 4.0 y 5.0.
- rds-ca-rsa2048-g1: utiliza una entidad de certificación con el algoritmo de clave privada RSA 2048 y el algoritmo de firma SHA256 en la mayoría de las regiones de AWS. Esta CA admite la rotación automática de certificados de servidor.
- rds-ca-rsa4096-g1: utiliza una entidad de certificación con el algoritmo de clave privada RSA 4096 y el algoritmo de firma SHA384. Esta CA admite la rotación automática de certificados de servidor.

> **Note**
>
> Si utiliza la AWS CLI, puede ver la validez de las entidades de certificación enumeradas anteriormente mediante describe-certificates.

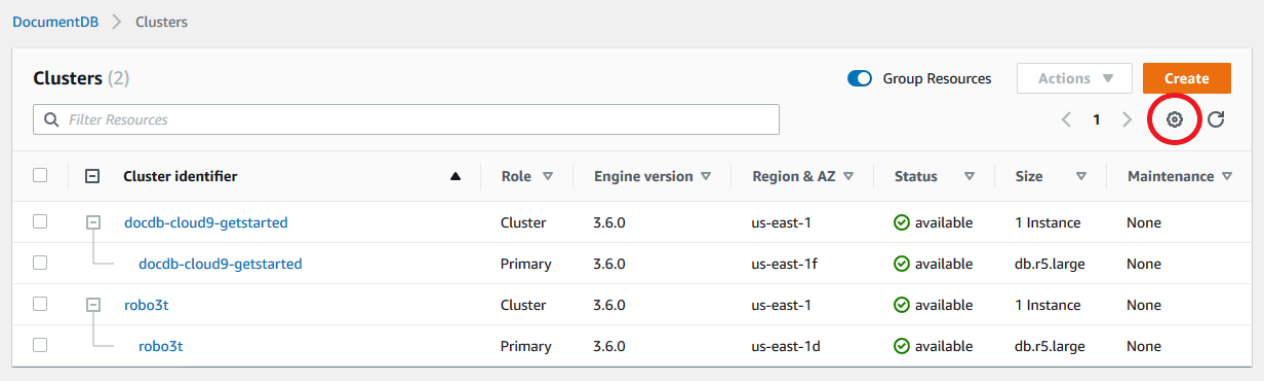
> **Note**
>
> Las instancias de Amazon DocumentDB 4.0 y 5.0 no requieren un reinicio.
> La actualización de las instancias de Amazon DocumentDB 3.6 requiere un reinicio, lo que podría causar una interrupción del servicio. Antes de actualizar el certificado de servidor, asegúrese de haber completado el paso 1.

Using the Consola de administración de AWS

Complete los pasos siguientes para identificar y rotar el certificado de servidor antiguo para las instancias de Amazon DocumentDB existentes mediante la Consola de administración de AWS.

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon DocumentDB en https://console.aws.amazon.com/docdb.
2. En la lista de regiones en la esquina superior derecha de la pantalla, seleccione la Región de AWS en la que residen sus clústeres.
3. En el panel de navegación en el lado izquierdo de la consola, en DAX, elija Clústeres.
4. Es posible que necesite identificar qué instancias siguen en el antiguo certificado de servidor (`rds-ca-2017`). Puede hacerlo en la columna Autoridad de certificación, que está oculta de forma predeterminada. Para mostrar la columna Certificate authority (Entidad de certificación), haga lo siguiente:

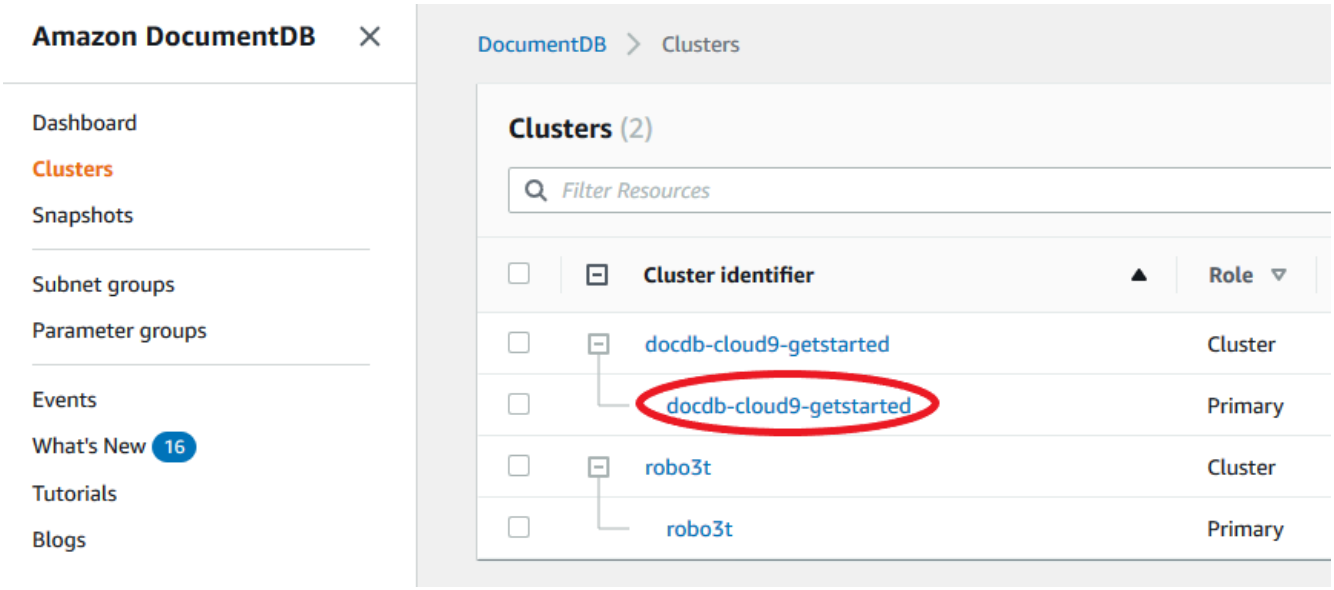
   a. Elija el icono Settings (Configuración).



   b. En la lista de columnas visibles, elija la columna Certificate authority (Entidad de certificación).

   c. Para guardar los cambios, seleccione Confirmar.

5. De nuevo en el cuadro de navegación de clústeres, verá la columna Identificador del clúster. Las instancias se muestran en clústeres, de forma similar a la siguiente captura de pantalla.



6. Marque la casilla de verificación situada a la izquierda de la instancia de su interés.
7. Elija Actions (Acciones) y después Modify (Modificar).
8. En Entidad de certificación, seleccione el nuevo certificado de servidor (`rds-ca-rsa2048-g1`, `rds-ca-rsa4096-g1` o `rds-ca-ecc384-g1`) para esta instancia.
9. Puede ver un resumen de los cambios en la página siguiente. Tenga en cuenta que se muestra una alerta adicional para recordarle que debe asegurarse de que su aplicación utilice el paquete más reciente de certificados de CA antes de modificar la instancia, con el fin de evitar que se interrumpa la conectividad.
10. Puede optar por aplicar la modificación durante el próximo periodo de mantenimiento o bien aplicarla de inmediato. Si su intención es modificar el certificado del servidor inmediatamente, utilice la opción Apply immediately (Aplicar inmediatamente).
11. Seleccione Modify instance (Modificar instancia) para completar la actualización.

Using the AWS CLI

Complete los pasos siguientes para identificar y rotar el certificado de servidor antiguo para las instancias de Amazon DocumentDB existentes mediante la AWS CLI.

1. Para modificar las instancias de inmediato, ejecute el siguiente comando para cada instancia del clúster. Use uno de los siguientes certificados: `rds-ca-rsa2048-g1`, `rds-ca-rsa4096-g1` o `rds-ca-ecc384-g1`.

```
aws docdb modify-db-instance --db-instance-identifier <yourInstanceIdentifier>
 --ca-certificate-identifier rds-ca-rsa4096-g1 --apply-immediately
```

2. Para modificar las instancias de los clústeres de tal forma que usen el nuevo certificado de CA durante el próximo periodo de mantenimiento del clúster, ejecute el siguiente comando para cada instancia del clúster. Use uno de los siguientes certificados: `rds-ca-rsa2048-g1`, `rds-ca-rsa4096-g1` o `rds-ca-ecc384-g1`.

```
aws docdb modify-db-instance --db-instance-identifier <yourInstanceIdentifier>
 --ca-certificate-identifier rds-ca-rsa4096-g1 --no-apply-immediately
```

Solución de problemas

Si tiene problemas para conectarse al clúster como parte de la rotación de certificados, le sugerimos lo siguiente:

- Reinicie sus instancias. Para rotar el nuevo certificado es necesario reiniciar cada una de las instancias. Si aplicó el nuevo certificado a una o más instancias pero no las reinició, reinícielas para aplicar el nuevo certificado. Para obtener más información, consulte Reinicio de la instancia de Amazon DocumentDB.
- Compruebe que sus clientes están utilizando el paquete de certificados más reciente. Consulte ¿Cómo puedo estar seguro de que estoy usando el paquete de CA más reciente?.
- Compruebe que las instancias están utilizando el certificado más reciente. Consulte ¿Cómo puedo saber cuáles de mis instancias de Amazon DocumentDB usan el certificado de servidor antiguo/nuevo?.
- Compruebe que la última entidad emisora de certificados está siendo utilizada por la aplicación. Algunos controladores, como Java y Go, requieren código adicional para importar varios certificados de un paquete de certificados al almacén de confianza. Para obtener más información sobre cómo conectarse a Amazon DocumentDB con TLS, consulte Conexión mediante programación a Amazon DocumentDB.
- Póngase en contacto con el soporte. Si tiene preguntas o problemas, póngase en contacto con Soporte.

Preguntas frecuentes

A continuación se presentan respuestas a algunas preguntas comunes acerca de los certificados TLS.

¿Qué hago si tengo preguntas o problemas?

Si tiene preguntas o problemas, póngase en contacto con Soporte.

¿Cómo sé si estoy usando TLS para conectarme a mi clúster de Amazon DocumentDB?

Para determinar si el clúster usa TLS, examine el parámetro `tls` del grupo de parámetros del clúster. Si el parámetro `tls` se encuentra establecido en `enabled`, está utilizando el certificado TLS para conectarse al clúster. Para obtener más información, consulte Administración de los grupos de parámetros de clúster de Amazon DocumentDB.

¿Por qué hay que actualizar los certificados de CA y de servidor?

Los certificados de CA y de servidor de Amazon DocumentDB se actualizaron de conformidad con las prácticas recomendadas de mantenimiento y seguridad estándar para Amazon DocumentDB. Los certificados de CA y de servidor actuales caducarán el miércoles 18 de mayo de 2022.

¿Qué sucede si no realizo ninguna acción antes de la fecha de caducidad?

Si utiliza TLS para conectarse al clúster de Amazon DocumentDB y no realiza el cambio antes del 18 de mayo de 2022, las aplicaciones que se conectan a través de TLS ya no podrán comunicarse más con el clúster de Amazon DocumentDB.

Amazon DocumentDB no rotará los certificados de la base de datos automáticamente antes de la fecha de caducidad. Debe actualizar las aplicaciones y los clústeres para utilizar los nuevos certificados de CA antes o después de la fecha de caducidad.

¿Cómo puedo saber cuáles de mis instancias de Amazon DocumentDB usan el certificado de servidor antiguo/nuevo?

Para identificar las instancias de Amazon DocumentDB que siguen utilizando el certificado de servidor antiguo, puede utilizar la Consola de administración de AWS o la AWS CLI de Amazon DocumentDB.

Uso de Consola de administración de AWS

Identificación de las instancias de los clústeres que utilizan el certificado anterior

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon DocumentDB en https://console.aws.amazon.com/docdb.

2. En la lista de regiones de la parte superior derecha de la pantalla, elija la Región de AWS en la que residen sus instancias.
3. En el panel de navegación del lado izquierdo de la consola, elija Instances (Instancias).
4. En la columna Entidad de certificación (oculta de forma predeterminada) se muestran las instancias que todavía contienen el certificado de servidor antiguo (`rds-ca-2017`) y el certificado de servidor nuevo (`rds-ca-rsa2048-g1`, `rds-ca-rsa4096-g1` o `rds-ca-ecc384-g1`). Para mostrar la columna Certificate authority (Entidad de certificación), haga lo siguiente:

   a. Elija el icono Settings (Configuración).

   b. En la lista de columnas visibles, elija la columna Certificate authority (Entidad de certificación).

   c. Para guardar los cambios, seleccione Confirmar.

Uso de AWS CLI

Para identificar las instancias de los clústeres que utilizan el certificado de servidor anterior, utilice el comando `describe-db-clusters` con lo siguiente.

```
aws docdb describe-db-instances \
    --filters Name=engine,Values=docdb \
    --query 'DBInstances[*].
{CertificateVersion:CACertificateIdentifier,InstanceID:DBInstanceIdentifier}'
```

¿Cómo puedo modificar instancias individuales de mi clúster de Amazon DocumentDB para actualizar el certificado de servidor?

Recomendamos actualizar al mismo tiempo los certificados de servidor de todas las instancias de un clúster determinado. Para modificar las instancias del clúster, puede utilizar la consola o la AWS CLI.

> **Note**
>
> La actualización de las instancias requiere un reinicio, lo que podría causar una interrupción del servicio. Antes de actualizar el certificado de servidor, asegúrese de haber completado el paso 1.

Uso de Consola de administración de AWS

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon DocumentDB en https://console.aws.amazon.com/docdb.
2. En la lista de regiones en la esquina superior derecha de la pantalla, seleccione la Región de AWS en la que residen sus clústeres.
3. En el panel de navegación del lado izquierdo de la consola, elija Instances (Instancias).
4. La columna (oculta de forma predeterminada) Certificate authority (Entidad de certificación) muestra las instancias que todavía contienen el certificado de servidor antiguo (`rds-ca-2017`). Para mostrar la columna Certificate authority (Entidad de certificación), haga lo siguiente:
   a. Elija el icono Settings (Configuración).
   b. En la lista de columnas visibles, elija la columna Certificate authority (Entidad de certificación).
   c. Para guardar los cambios, seleccione Confirmar.
5. Seleccione una instancia que desee modificar.
6. Elija Actions (Acciones) y después Modify (Modificar).
7. En Entidad de certificación, seleccione uno de los nuevos certificados de servidor (`rds-ca-rsa2048-g1`, `rds-ca-rsa4096-g1` o `rds-ca-ecc384-g1`) para esta instancia.
8. Puede ver un resumen de los cambios en la página siguiente. Tenga en cuenta que se muestra una alerta adicional para recordarle que debe asegurarse de que su aplicación utilice el paquete más reciente de certificados de CA antes de modificar la instancia, con el fin de evitar que se interrumpa la conectividad.
9. Puede optar por aplicar la modificación durante el próximo periodo de mantenimiento o bien aplicarla de inmediato.
10. Seleccione Modify instance (Modificar instancia) para completar la actualización.

Uso de AWS CLI

Complete los pasos siguientes para identificar y rotar el certificado de servidor antiguo para las instancias de Amazon DocumentDB existentes mediante la AWS CLI.

1. Para modificar las instancias de inmediato, ejecute el siguiente comando para cada instancia del clúster.

```
aws docdb modify-db-instance --db-instance-identifier <yourInstanceIdentifier> --
ca-certificate-identifier rds-ca-rsa4096-g1 --apply-immediately
```

2. Para modificar las instancias de los clústeres de tal forma que usen el nuevo certificado de CA durante el próximo periodo de mantenimiento del clúster, ejecute el siguiente comando para cada instancia del clúster.

```
aws docdb modify-db-instance --db-instance-identifier <yourInstanceIdentifier> --
ca-certificate-identifier rds-ca-rsa4096-g1 --no-apply-immediately
```

¿Qué sucede si añado una nueva instancia a un clúster existente?

Todas las instancias nuevas que se creen utilizan el certificado de servidor antiguo y requieren conexiones TLS que usen el certificado de CA antiguo. Cualquier instancia nueva de Amazon DocumentDB creada después del 21 de marzo de 2022 utilizará de forma predeterminada los certificados nuevos.

¿Qué sucede si se sustituye una instancia o se produce una conmutación por error en el clúster?

Si se sustituye una instancia en el clúster, la nueva instancia que se crea continúa usando el mismo certificado de servidor que se estaba utilizando anteriormente. Se recomienda actualizar los certificados de servidor para todas las instancias al mismo tiempo. Si se produce una conmutación por error en el clúster, se usará el certificado de servidor del nuevo nodo principal.

Si no uso TLS para conectarme al clúster, ¿tengo que actualizar todas las instancias?

Si no usa TLS para conectarse a los clústeres de Amazon DocumentDB, no es necesaria ninguna acción.

Si no estoy usando TLS para conectarme a mi clúster pero tengo previsto hacerlo en el futuro, ¿qué tengo que hacer?

Si creó un clúster antes del 21 de marzo de 2022, siga el paso 1 y el paso 2 de la sección anterior para asegurarse de que la aplicación utiliza la agrupación de CA actualizada y de que cada instancia de Amazon DocumentDB utiliza el certificado de servidor más reciente. Si creó un clúster después del 21 de marzo de 2022, el clúster ya tendrá el certificado de servidor más reciente. Para comprobar que la aplicación utiliza el grupo de CA más reciente, consulte Si no uso TLS para conectarme al clúster, ¿tengo que actualizar todas las instancias?

¿Puede prorrogarse el plazo más allá del 18 de mayo de 2022?

Si sus aplicaciones se conectan a través de TLS, la fecha límite no se podrá prorrogar más allá del 18 de mayo de 2022.

¿Cómo puedo estar seguro de que estoy usando el paquete de CA más reciente?

Por razones de compatibilidad, los archivos de los paquetes de CA antiguos y nuevos llevan el nombre `us-gov-west-1-bundle.pem`. También puede usar herramientas como `openssl` o `keytool` para inspeccionar el paquete de CA.

¿Por qué veo “RDS” en el nombre del paquete de CA?

Para determinadas funciones de administración, como la administración de certificados, Amazon DocumentDB utiliza tecnología operativa que se comparte con Amazon Relational Database Service (Amazon RDS).

¿Cuándo caduca el nuevo certificado?

El nuevo certificado del servidor caducará (por lo general) de la siguiente manera:

- rds-ca-rsa2048-g1: caduca en 2061
- rds-ca-rsa4096-g1: caduca en 2121
- rds-ca-ecc384-g1: caduca en 2121

¿Qué tipo de errores veré si no tomo medidas antes de que caduque el certificado?

Los mensajes de error variarán en función del controlador. En general, verá errores de validación de certificados que contienen la cadena “el certificado ha caducado”.

Si he aplicado el nuevo certificado de servidor, ¿puedo revertirlo al certificado de servidor antiguo?

Si necesita revertir una instancia al certificado de servidor antiguo, recomendamos que haga lo mismo para todas las instancias del clúster. Puede revertir el certificado de servidor para cada instancia de un clúster mediante la Consola de administración de AWS o la AWS CLI.

Uso de Consola de administración de AWS

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon DocumentDB en https://console.aws.amazon.com/docdb.
2. En la lista de regiones en la esquina superior derecha de la pantalla, seleccione la Región de AWS en la que residen sus clústeres.
3. En el panel de navegación del lado izquierdo de la consola, elija Instances (Instancias).
4. Seleccione una instancia que desee modificar. Elija Actions (Acciones) y después Modify (Modificar).
5. En Autoridad de certificación, puede seleccionar el certificado de servidor antiguo (`rds-ca-2017`).
6. Elija Continue (Continuar) para ver un resumen de las modificaciones.
7. En la página que aparece, puede elegir programar las modificaciones para que se apliquen en el próximo periodo de mantenimiento o aplicar las modificaciones inmediatamente. Realice la selección y elija Modify instance (Modificar instancia).

> **Note**
>
> Si opta por aplicar las modificaciones inmediatamente, también se aplican los cambios de la cola de modificaciones pendientes. Si alguna de las modificaciones pendientes requiere un tiempo de inactividad, elegir esta opción puede provocar un tiempo de inactividad inesperado.

Uso de AWS CLI

```
aws docdb modify-db-instance --db-instance-identifier <db_instance_name> ca-
certificate-identifier rds-ca-2017 <--apply-immediately | --no-apply-immediately>
```

Si elige `--no-apply-immediately`, los cambios se aplicarán durante el próximo periodo de mantenimiento del clúster.

Si restauro a partir de una instantánea o de una restauración puntual, ¿tendrá el nuevo certificado de servidor?

Si restaura una instantánea o realiza una restauración puntual después del 21 de marzo de 2022, el nuevo clúster que se crea utilizará el nuevo certificado de entidad de certificación.

¿Qué sucede si tengo problemas para conectarme directamente a mi clúster de Amazon DocumentDB desde Mac OS X Catalina?

Mac OS X Catalina ha actualizado los requisitos para certificados de confianza. Ahora los certificados de confianza deben tener una validez de 825 días o menos (consulte https://support.apple.com/en-us/HT210176). Los certificados de instancia de Amazon DocumentDB son válidos durante más de cuatro años, más que el máximo de Mac OS X. Para conectarse directamente a un clúster de Amazon DocumentDB desde un equipo que ejecuta Mac OS X Catalina, debe permitir certificados no válidos al crear la conexión TLS. En este caso, los certificados no válidos significan que el período de validez es superior a 825 días. Debe comprender los riesgos antes de permitir certificados no válidos al conectarse al clúster de Amazon DocumentDB.

Para conectarse a un clúster de Amazon DocumentDB desde OS X Catalina utilizando la AWS CLI, utilice el parámetro `tlsAllowInvalidCertificates`.

```
mongo --tls --host <hostname> --username <username> --password <password> --port 27017
 --tlsAllowInvalidCertificates
```

Validación de la conformidad en Amazon DocumentDB

Auditores externos evalúan la seguridad y la conformidad de Amazon DocumentDB como parte de varios programas de conformidad de AWS, incluidos los siguientes:

- Controles del Sistema y Organizaciones (System and Organization Controls, SOC) 1, 2 y 3. Para obtener más información, consulte SOC.
- Programa Federal de Administración de Riesgos y Autorizaciones (FedRAMP). Para obtener más información, consulte Servicios de AWS en el ámbito del programa de conformidad.
- Estándar de Seguridad de Datos del Sector de las Tarjetas de Pago (PCI DSS, Payment Card Industry Data Security Standard). Para obtener más información, consulte PCI DSS.

- ISO 9001, 27001, 27017 y 27018. Para obtener más información, consulte Certificado ISO.
- Acuerdo para socio empresarial de la ley de portabilidad y responsabilidad de seguros médicos (HIPAA BAA). Para obtener más información, consulte Conformidad con HIPAA.

AWS proporciona una lista actualizada frecuentemente de los servicios de AWS adscritos al ámbito de los programas de conformidad en Servicios de AWS en el ámbito del programa de conformidad.

Los informes de auditoría de terceros están disponibles para su descarga mediante AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact.

Para obtener más información acerca de los programas de conformidad de AWS, consulte Programas de conformidad de AWS.

Su responsabilidad de conformidad al utilizar Amazon DocumentDB se determina en función de la sensibilidad de los datos, los objetivos de conformidad de la organización, así como de la legislación y los reglamentos aplicables. Si su uso de Amazon DocumentDB está sujeto a conformidad con ciertos estándares, como HIPAA o PCI, AWS proporciona recursos de ayuda:

- Recursos de conformidad de AWS: un conjunto de manuales y guías que podría aplicarse a su sector y ubicación.
- Guías de inicio rápido de seguridad y conformidad: guías de implementación que incluyen consideraciones sobre arquitectura y ofrecen pasos para implementar entornos de referencia centrados en la seguridad y la conformidad en AWS.
- AWS Config: un servicio que evalúa en qué medida las configuraciones de los recursos cumplen las prácticas internas, las directrices del sector y las normativas.
- AWS Security Hub: un servicio que ofrece una vista integral de su estado de seguridad en AWS que le ayuda a verificar la conformidad con los estándares del sector de seguridad y las prácticas recomendadas.
- Documento técnico sobre el diseño de arquitecturas para cumplir los requisitos de seguridad y conformidad de HIPAA: documento técnico en el que se describe cómo las empresas pueden utilizar AWS para crear aplicaciones conformes con HIPAA.

Resiliencia de Amazon DocumentDB

La infraestructura global de AWS se divide en Regiones de AWS y zonas de disponibilidad. Las Regiones de AWS proporcionan varias zonas de disponibilidad físicamente independientes

y aisladas que se encuentran conectadas mediante redes con un alto nivel de rendimiento y redundancia, además de baja latencia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre zonas de disponibilidad sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de centros de datos únicos o múltiples.

Un clúster de base de Amazon DocumentDB solo se puede crear en una Amazon VPC que tenga un mínimo de dos subredes en al menos dos zonas de disponibilidad. Mediante la distribución de las instancias del clúster en al menos dos zonas de disponibilidad, Amazon DocumentDB contribuye a garantizar que haya instancias disponibles en el clúster de base de datos en el caso improbable de que se produzca un error en una zona de disponibilidad. El volumen de un clúster de base de datos de Amazon DocumentDB siempre abarca tres zonas de disponibilidad. De este modo, se proporciona un almacenamiento duradero y con un menor riesgo de pérdida de datos.

Para obtener más información sobre las Regiones de AWS y las zonas de disponibilidad, consulte Infraestructura global de AWS.

Además de la infraestructura global de AWS, Amazon DocumentDB ofrece varias características que lo ayudan con sus necesidades de resiliencia y copia de seguridad de los datos.

Almacenamiento con recuperación automática y tolerancia a errores

: Cada porción de 10 GB del volumen de almacenamiento se replica de seis maneras, en tres zonas de disponibilidad. Amazon DocumentDB utiliza un almacenamiento tolerante a errores que gestiona de forma transparente la pérdida de hasta dos copias de datos sin que ello afecte a la disponibilidad de escritura de la base de datos y de hasta tres copias sin que ello afecte a la disponibilidad de lectura. El almacenamiento de Amazon DocumentDB también se recupera automáticamente; los bloques de datos y los discos se escanean continuamente para detectar errores y se sustituyen automáticamente.

Copias de seguridad y restauración manuales

: Amazon DocumentDB ofrece la capacidad de crear copias de seguridad completas de su clúster para retención y recuperación a largo plazo. Para obtener más información, consulte Copia de seguridad y restauración en Amazon DocumentDB.

Recuperación a un momento dado

: La recuperación a un momento dado ayuda a proteger los clústeres de Amazon DocumentDB de operaciones accidentales de escritura o eliminación. Al habilitar la recuperación a un momento

dado, ya no hay que preocuparse por crear, mantener o planificar copias de seguridad bajo demanda. Para obtener más información, consulte Restauración a un momento dado.

Seguridad de la infraestructura en Amazon DocumentDB

Como servicio administrado, Amazon DocumentDB está protegido por una seguridad de red global de AWS. Para obtener información sobre los servicios de seguridad de AWS y sobre cómo AWS protege la infraestructura, consulte Seguridad en la nube de AWS. Para diseñar su entorno de AWS siguiendo las prácticas recomendadas de seguridad de infraestructura, consulte Protección de la infraestructura en Portal de seguridad de AWS Well-Architected Framework.

Puede utilizar llamadas a la API publicadas en AWS para acceder a Amazon DocumentDB a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con confidencialidad directa total (PFS) como DHE (Ephemeral Diffie-Hellman) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Puede llamar a estas operaciones de la API desde cualquier ubicación de red. Puede utilizar políticas de Amazon DocumentDB para controlar el acceso desde puntos de conexión específicos de Amazon Virtual Private Cloud (Amazon VPC) o VPC específicas. Este proceso aísla con eficacia el acceso de red a un recurso de Amazon DocumentDB determinado únicamente desde la VPC específica de la red de AWS.

> **Note**
>
> Amazon DocumentDB no admite políticas de acceso basadas en recursos.

API de Amazon DocumentDB y puntos de conexión de VPC de interfaz (AWS PrivateLink)

> **Note**
>
> Los clústeres elásticos de Amazon DocumentDB no admiten puntos de conexión de VPC de AWS PrivateLink.

Puede establecer una conexión privada entre los puntos de conexión de VPC y la API de Amazon DocumentDB mediante la creación de un punto de conexión de VPC de interfaz. Puntos de enlace de tipo interfaz con tecnología de AWS PrivateLink.

Si bien los clústeres basados en instancias de Amazon DocumentDB no requieren una conexión de puntos de conexión de VPC de interfaz, AWS PrivateLink le permite acceder de forma privada a las operaciones de la API de Amazon DocumentDB sin una puerta de enlace de Internet, un dispositivo NAT, una conexión VPN ni una conexión de Direct Connect. Las instancias de Amazon DocumentDB de su VPC no necesitan direcciones IP públicas para comunicarse con los puntos de conexión de la API de Amazon DocumentDB para lanzar, modificar o terminar instancias de base de datos y clústeres de base de datos. Las instancias de Amazon DocumentDB tampoco necesitan direcciones IP públicas para utilizar ninguna de las operaciones de la API de Amazon DocumentDB disponibles. El tráfico entre la VPC y Amazon DocumentDB no sale de la red de Amazon.

Cada punto de conexión de la interfaz está representado por una o más interfaces de red elásticas en las subredes. Para obtener más información, consulte Interfaces de red elásticas en la Guía del usuario de Amazon EC2.

Para obtener más información sobre los puntos de conexión de VPC, consulte Acceda a un Servicio de AWS mediante un punto de conexión de VPC de interfaz en la Guía del usuario de Amazon Virtual Private Cloud (AWS PrivateLink). Para obtener más información sobre las operaciones de Amazon DocumentDB, consulte Referencia de la API para la administración de recursos, instancias y clústeres de Amazon DocumentDB.

Temas

- Consideraciones para los puntos de enlace de VPC
- Disponibilidad por región
- Creación de un punto de conexión de VPC de interfaz para la API de Amazon DocumentDB

- Creación de una política de punto de conexión de VPC para la API de Amazon DocumentDB

Consideraciones para los puntos de enlace de VPC

Antes de configurar un punto de conexión de VPC de tipo interfaz para los puntos de conexión de la API de Amazon DocumentDB, asegúrese de revisar los requisitos previos del puntos de conexión de interfaz en la Guía del usuario de nube privada virtual (AWS PrivateLink) de Amazon.

Todas las operaciones de API de Amazon DocumentDB pertinentes de la administración de recursos de Amazon DocumentDB están disponibles desde la VPC mediante el uso de AWS PrivateLink.

Las políticas de puntos de conexión de VPC son compatibles con los puntos de conexión de API de Amazon DocumentDB. De forma predeterminada, se permite el acceso completo a las operaciones de API de Amazon DocumentDB a través del punto de conexión. Para obtener más información, consulte Uso de políticas de punto de conexión para controlar el acceso a puntos de conexión de VPC en la Guía del usuario de Amazon Virtual Private Cloud (AWS PrivateLink).

Disponibilidad por región

La API de Amazon DocumentDB actualmente admite puntos de conexión de VPC en las siguientes Regiones de AWS:

- Este de EE. UU. (Ohio)
- Este de EE. UU. (Norte de Virginia)
- Oeste de EE. UU. (Oregón)
- África (Ciudad del Cabo)
- Asia-Pacífico (Hong Kong)
- Asia-Pacífico (Mumbai)
- Asia-Pacífico (Hyderabad)
- Asia-Pacífico (Osaka)
- Asia-Pacífico (Seúl)
- Asia-Pacífico (Singapur)
- Asia-Pacífico (Sídney)
- Asia-Pacífico (Tokio)
- Canadá (centro)

- China (Pekín)
- China (Ningxia)
- Europa (Fráncfort)
- Europa (Irlanda)
- Europa (Londres)
- Europa (París)
- Europa (España)
- Europa (Milán)
- Oriente Medio (EAU)
- América del Sur (São Paulo)
- AWS GovCloud (Este de EE. UU.)
- AWS GovCloud (Oeste de EE. UU.)

Creación de un punto de conexión de VPC de interfaz para la API de Amazon DocumentDB

Puede crear un punto de conexión de VPC para la API de Amazon DocumentDB mediante la consola de Amazon VPC o desde la AWS Command Line Interface (AWS CLI). Para obtener más información, consulte Acceda a un Servicio de AWS mediante un punto de conexión de VPC de interfaz en la Guía del usuario de Amazon Virtual Private Cloud (AWS PrivateLink).

Cree un punto de conexión de VPC para la API de Amazon DocumentDB mediante el uso del nombre del servicio `com.amazonaws.region.rds`.

Excepto en las Regiones de AWS de China, si habilita un DNS privado para el punto de conexión, podrá hacer solicitudes de la API a Amazon DocumentDB con el punto de conexión de VPC mediante el nombre de DNS predeterminado para las Regiones de AWS, como rds.us-east-1.amazonaws.com. En las Regiones de AWS de China (Pekín) y China (Ningxia), puede llevar a cabo solicitudes de la API con el punto de conexión de VPC mediante rds-api.cn-north-1.amazonaws.com.cn y rds-api.cn-northwest-1.amazonaws.com.cn, respectivamente.

Para obtener más información, consulte Acceda a un Servicio de AWS mediante un punto de conexión de VPC de interfaz en la Guía del usuario de Amazon Virtual Private Cloud (AWS PrivateLink).

Creación de una política de punto de conexión de VPC para la API de Amazon DocumentDB

Puede asociar una política de punto de conexión al punto de conexión de VPC que controla el acceso a la API de Amazon DocumentDB. La política especifica la siguiente información:

- La entidad principal que puede realizar acciones.
- Las acciones que se pueden realizar.
- Los recursos en los que se pueden llevar a cabo las acciones.

Para obtener más información, consulte Uso de políticas de punto de conexión para controlar el acceso a puntos de conexión de VPC en la Guía del usuario de Amazon Virtual Private Cloud (AWS PrivateLink).

Ejemplo: política de punto de conexión de VPC para acciones de la API de Amazon DocumentDB

A continuación, se muestra un ejemplo de una política de punto de conexión para la API de Amazon DocumentDB. Cuando se asocia a un punto de conexión, esta política concede acceso a las acciones de la API de Amazon DocumentDB enumeradas para todas las entidades principales de todos los recursos.

```
{
"Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "docdb:CreateDBInstance",
            "docdb:ModifyDBInstance",
            "docdb:CreateDBSnapshot"
         ],
         "Resource":"*"
      }
   ]
}
```

Ejemplo: política de punto de enlace de la VPC que deniega todo el acceso desde una cuenta de AWS especificada

La siguiente política de punto de conexión de VPC deniega a la cuenta de AWS 123456789012 todo el acceso a los recursos mediante el punto de conexión. La política permite todas las acciones de otras cuentas.

```
{
  "Statement": [
    {
      "Action": "*",
      "Effect": "Allow",
      "Resource": "*",
      "Principal": "*"
    },
    {
      "Action": "*",
      "Effect": "Deny",
      "Resource": "*",
      "Principal": { "AWS": [ "123456789012" ] }
     }
   ]
}
```

Prácticas recomendadas de seguridad para Amazon DocumentDB

Para las prácticas recomendadas de seguridad, debe usar cuentas de (IAM) de AWS Identity and Access Management para controlar el acceso a las operaciones de la API de Amazon DocumentDB, especialmente las operaciones que crean, modifican o eliminan recursos de . Dichos recursos incluyen clústeres, grupos de seguridad y grupos de parámetros. Debe utilizar también IAM para controlar las acciones administrativas comunes como la restauración de las copias de seguridad de los clústeres. Al crear roles de IAM, utilice el principio de privilegios mínimos.

- Imponga privilegios mínimos con control de acceso basado en roles.
- Asigne una cuenta de IAM individual a cada persona que administre los recursos de Amazon DocumentDB. No utilice el usuario raíz de Cuenta de AWS para administrar los recursos de Amazon DocumentDB. Cree un usuario de IAM para todos, incluido usted mismo.
- Conceda a cada usuario el conjunto mínimo de permisos requerido para realizar sus tareas.
- Use los grupos de IAM para administrar con eficacia los permisos para varios usuarios. Para obtener más información acerca de IAM, consulte la Guía del usuario de IAM. Para obtener información sobre las prácticas recomendadas de IAM, consulte Prácticas recomendadas de IAM.

- Rote con regularidad sus credenciales de IAM.
- Configure AWS Secrets Manager para rotar automáticamente los secretos de Amazon DocumentDB. Para obtener más información, consulte Rotación de sus secretos de AWS Secrets Manager y Rotación de secretos de Amazon DocumentDB en la Guía del usuario de AWS Secrets Manager.
- Utilice seguridad de la capa de transporte (TLS) y el cifrado en reposo para cifrar los datos.

Auditoría de eventos de Amazon DocumentDB

Con Amazon DocumentDB (con compatibilidad con MongoDB), puede auditar eventos que se realizaron en su clúster. Los intentos de autenticación correctos e incorrectos, la eliminación de una colección en una base de datos o la creación de un índice son algunos ejemplos de eventos registrados. De forma predeterminada, la auditoría está deshabilitada en Amazon DocumentDB y, para utilizar esta característica, es necesario suscribirse.

Cuando la auditoría está habilitada, Amazon DocumentDB registra los eventos de lenguaje de definición de datos (DDL), lenguaje de manipulación de datos (DML), autenticación, autorización y administración de usuarios en Amazon Logs. CloudWatch Cuando la auditoría está habilitada, Amazon DocumentDB exporta los registros de auditoría del clúster (documentos JSON) a Amazon CloudWatch Logs. Puede utilizar Amazon CloudWatch Logs para analizar, supervisar y archivar sus eventos de auditoría de Amazon DocumentDB.

Aunque Amazon DocumentDB no cobra ningún coste adicional por habilitar la auditoría, se le cobran tarifas estándar por el uso de CloudWatch Logs. Para obtener información sobre CloudWatch los precios de Logs, consulta CloudWatch los precios de Amazon.

La función de auditoría de Amazon DocumentDB es claramente diferente del uso de los recursos de servicio con el que se supervisa. AWS CloudTrail CloudTrail registra las operaciones que se realizan con AWS Command Line Interface (AWS CLI) o Consola de administración de AWS en recursos como clústeres, instancias, grupos de parámetros e instantáneas. La auditoría de los recursos CloudTrail está activada de forma predeterminada y no se puede deshabilitar. La característica de auditoría de Amazon DocumentDB es opcional. Registra las operaciones que tienen lugar dentro del clúster en los distintos objetos, como, por ejemplo, bases de datos, colecciones, índices y usuarios.

Temas

- Eventos admitidos
- Habilitación de auditorías

- Deshabilitación de auditorías
- Acceso a los eventos de auditoría
- Filtrado de eventos de auditoría de DML

Eventos admitidos

La auditoría de Amazon DocumentDB admite las siguientes categorías de eventos:

- Lenguaje de definición de datos (DDL): incluye las operaciones de administración de bases de datos, las conexiones, la administración de usuarios y la autorización.
- Eventos de lectura del lenguaje de manipulación de datos (lecturas DML): incluye `find()` y los distintos operadores de agregación, operadores aritméticos, operadores booleanos y otros operadores de consulta de lectura.
- Eventos de escritura del lenguaje de manipulación de datos (escrituras en DML): incluye operadores `insert(), update(), delete(),` y `bulkWrite()`

Los tipos de eventos son los siguientes.

Tipo de evento	Categoría	Description (Descripción)
`authCheck`	Autorización	Código de resultado 0: éxito
		Código de resultado 13: intentos no autorizados de realizar una operación.
`authenticate`	Connection	Intentos de autenticación correctos e incorrectos en una nueva conexión.

Tipo de evento	Categoría	Description (Descripción)
`auditConfigure`	DDL	Auditoría de la configuración de filtrado.
`createDatabase`	DDL	Creación de una nueva base de datos.
`createCollection`	DDL	Creación de una nueva colección en una base de datos.
`createIndex`	DDL	Creación de un nuevo índice en una colección.
`dropCollection`	DDL	Eliminación de una nueva colección en una base de datos.
`dropDatabase`	DDL	Eliminación de una base de datos.
`dropIndex`	DDL	Eliminación de un índice en una colección.
`modifyChangeStreams`	DDL	Se creó el flujo de cambios.
`renameCollection`	DDL	Renombrar una nueva colección en una base de datos.
`createRole`	Administración de roles	Creación de un rol.

Tipo de evento	Categoría	Description (Descripción)
dropAllRolesFromDatabase	Administración de roles	Eliminación de todos los roles en una base de datos.
dropRole	Administración de roles	Descartando un rol.
grantPrivilegesToRole	Administración de roles	Concediendo privilegios a un rol.
grantRolesToRole	Administración de roles	Concediendo roles a un rol definido por el usuario.
revokePrivilegesFromRole	Administración de roles	Revocando los privilegios de un rol.
revokeRolesFromRole	Administración de roles	Revocando roles de un rol definido por el usuario.
updateRole	Administración de roles	Actualización de un rol.
createUser	Administración de usuarios	Creación de un nuevo usuario.
dropAllUsersFromDatabase	Administración de usuarios	Eliminación de todos los usuarios en una base de datos.
dropUser	Administración de usuarios	Eliminación de un usuario existente.
grantRolesToUser	Administración de usuarios	Concesión de roles a un usuario.

Tipo de evento	Categoría	Description (Descripción)
`revokeRolesFromUser`	Administración de usuarios	Revocando roles de un usuario.
`updateUser`	UserManagement	Actualización de un usuario existente.
`insert`	Escritura DML	Inserta uno o varios documentos en una colección.
`delete`	Escritura DML	Elimina uno o varios documentos de una colección.
`update`	Escritura DML	Modifica uno o varios documentos existentes en una colección.
`bulkWrite`	Escritura DML	Realiza múltiples operaciones de escritura con controles para determinar el orden de ejecución.
`setAuditConfig`	Escritura DML	Establezca un filtro nuevo para la auditoría de DML.
`count`	Lectura de DML	Devuelve el recuento de documentos que coincidirían con una consulta find() de la colección o vista.

Tipo de evento	Categoría	Description (Descripción)
`countDocuments`	Lectura de DML	Devuelve el recuento de documentos que coinciden con una consulta para una colección o vista.
`find`	Lectura de DML	Selecciona los documentos de una colección o vista y devuelve el cursor a los documentos seleccionados.
`getAuditConfig`	Lectura de DML	Recupere el filtro actual para la auditoría de DML.
`findAndModify`	Lectura de DML y escritura de DML	Modifica y devuelve un único documento.
`findOneAndDelete`	Lectura de DML y escritura de DML	Elimina un solo documento en función de los criterios de filtro y clasificación y devuelve el documento eliminado.
`findOneAndReplace`	Lectura de DML y escritura de DML	Sustituye un único documento en función del filtro especificado.
`findOneAndUpdate`	Lectura de DML y escritura de DML	Actualiza un único documento en función de los criterios de filtrado y clasificación.

Tipo de evento	Categoría	Description (Descripción)
`aggregate`	Lectura de DML y escritura de DML	Es compatible con APIs la canalización de agregación.
`distinct`	Lectura de DML	Busca los valores distintos de un campo especificado en una sola colección o vista y devuelve los resultados en una matriz.

> **Note**
>
> Los valores del campo de parámetros del documento de eventos de DML tienen un límite de tamaño de 1 KB. Amazon DocumentDB trunca el valor si supera 1 KB.

> **Note**
>
> Los eventos de eliminación de TTL no se auditan en este momento.

Habilitación de auditorías

Para habilitar la auditoría en un clúster, hay que seguir un proceso de dos pasos. Asegúrese de completar ambos pasos o los registros de auditoría no se enviarán a CloudWatch Logs.

Paso 1. Habilitación del parámetro de clúster audit_logs

Para habilitar la auditoría, debe modificar el parámetro `audit_logs` en el grupo de parámetros. `audit_logs` es una lista delimitada por comas de los eventos que se deben registrar. Los eventos se deben especificar en minúsculas y no debe haber espacios en blanco entre los elementos de la lista.

Puede especificar los siguientes valores para el grupo de parámetro:

Valor	Description (Descripción)	
`ddl`	Al configurarlo, se habilitará la auditoría de eventos DDL como CreateDatabase, DropDatabase, CreateCollection, DropCollection, CreateIndex, DropIndex, AuthCheck, authenticate, CreateUser, DropUser, User, User, UpdateUser y grantRolesTo revokeRolesFrom dropAllUsers FromDatabase	
`dml_read`	Cuando configura esto, se habilita la auditoría de eventos de lectura de DML como find, sort count, distinct, group, projecta, unwind, geoNear, geoIntersects, geoWithin y otros operadores de consulta de lectura de MongoDB.	

Valor	Description (Descripción)	
`dml_write`	Al configurarlo, se habilitará la auditoría de eventos de escritura de DML como insert(), update(), delete() y bulkWrite()	
`all`	Al configurarlo, se habilitará la auditoría de los eventos de la base de datos, como las consultas de lectura y escritura, las acciones de la base de datos y las acciones del administrador.	
`none`	Si lo configura, se deshabilitará la auditoría	

Valor	Description (Descripción)	
`enabled` (heredado)	Se trata de una configuración de parámetros antigua que equivale a “ddl”. Al configurarlo, se habilitará la auditoría de eventos DDL como CreateDatabase, DropDatabase, CreateCollection, DropCollection, CreateIndex, DropIndex, AuthCheck, authenticate, CreateUser, DropUser, User, User, UpdateUser y. grantRolesTo revokeRolesFrom dropAllUsersFromDatabase No se recomienda utilizar este ajuste porque se trata de un ajuste heredado.	

Valor	Description (Descripción)	
`disabled` (heredado)	Se trata de una configuración de parámetros antigua que equivale a “none”. No se recomienda utilizar este ajuste porque se trata de un ajuste heredado.	

> **Note**
>
> El valor predeterminado del parámetro de clúster audit_logs es none (“`disabled`” heredado).

También puede utilizar los valores mencionados anteriormente en combinaciones.

Valor	Description (Descripción)	
`ddl, dml_read`	Si lo configura, se habilitará la audición de los eventos DDL y los eventos de lectura de DML.	
`ddl, dml_write`	Si lo configura, se habilitará la audición de los eventos DDL y la lectura de DML.	

Valor	Description (Descripción)	
`dml_read, dml_write`	Si lo configura, se habilitará la audición de los eventos DDL	

> **Note**
>
> No es posible modificar un grupo de parámetros predeterminado.

Para obtener más información, consulte los siguientes temas:

- Creación de grupos de parámetros de clúster de Amazon DocumentDB

  Después de crear un grupo de parámetros, para modificarlo, debe cambiar el valor del parámetro `audit_logs` a `all`.
- Modificación de grupos de parámetros de clúster de Amazon DocumentDB

Paso 2. Habilitar la exportación CloudWatch de Amazon Logs

Si el valor del parámetro de `audit_logs` clúster es`enabled`,`ddl`, o `dml_read`dml_write, también debe habilitar Amazon DocumentDB para exportar los registros a Amazon. CloudWatch Si omite alguno de estos pasos, no se enviarán los registros de auditoría a. CloudWatch

Al crear un clúster, realizar una point-in-time-restore instantánea o restaurar una instantánea, puede habilitar CloudWatch los registros siguiendo estos pasos.

Using the Consola de administración de AWS

Para permitir que Amazon DocumentDB exporte registros CloudWatch mediante la consola, consulte los siguientes temas:

- Al crear un clúster: en Crear un clúster y una instancia principal mediante Consola de administración de AWS, consulte Creación de un clúster: configuraciones adicionales (paso 5, Exportaciones de registros)

- Al modificar un clúster existente — Modificación de un clúster de Amazon DocumentDB
- Al realizar una restauración de una instantánea de un clúster — Restauración de una instantánea del clúster
- Al realizar una point-in-time restauración: Restauración a un momento dado

Using the AWS CLI

Para habilitar los registros de auditoría al crear un nuevo clúster

El siguiente código crea el clúster `sample-cluster` y habilita los registros CloudWatch de auditoría.

Example

Para Linux, macOS o Unix:

```
aws docdb create-db-cluster \
    --db-cluster-identifier sample-cluster \
    --port 27017 \
    --engine docdb \
    --master-username master-username \
    --master-user-password password \
    --db-subnet-group-name default \
    --enable-cloudwatch-logs-exports audit
```

Para Windows:

```
aws docdb create-db-cluster ^
    --db-cluster-identifier sample-cluster ^
    --port 27017 ^
    --engine docdb ^
    --master-username master-username ^
    --master-user-password password ^
    --db-subnet-group-name default ^
    --enable-cloudwatch-logs-exports audit
```

Para habilitar los registros de auditoría al modificar un clúster existente

El siguiente código modifica el clúster `sample-cluster` y habilita los registros de CloudWatch auditoría.

Example

Para Linux, macOS o Unix:

```
aws docdb modify-db-cluster \
   --db-cluster-identifier sample-cluster \
   --cloudwatch-logs-export-configuration '{"EnableLogTypes":["audit"]}'
```

Para Windows:

```
aws docdb modify-db-cluster ^
   --db-cluster-identifier sample-cluster ^
   --cloudwatch-logs-export-configuration '{"EnableLogTypes":["audit"]}'
```

El resultado de estas operaciones será similar al que se indica a continuación (formato JSON).

```
{
    "DBCluster": {
        "HostedZoneId": "ZNKXH85TT8WVW",
        "StorageEncrypted": false,
        "DBClusterParameterGroup": "default.docdb4.0",
        "MasterUsername": "<user-name>",
        "BackupRetentionPeriod": 1,
        "Port": 27017,
        "VpcSecurityGroups": [
            {
                "Status": "active",
                "VpcSecurityGroupId": "sg-77186e0d"
            }
        ],
        "DBClusterArn": "arn:aws:rds:us-east-1:900083794985:cluster:sample-cluster",
        "Status": "creating",
        "Engine": "docdb",
        "EngineVersion": "4.0.0",
        "MultiAZ": false,
        "AvailabilityZones": [
            "us-east-1a",
            "us-east-1c",
            "us-east-1f"
        ],
        "DBSubnetGroup": "default",
        "DBClusterMembers": [],
```

```
        "ReaderEndpoint": "sample-cluster.cluster-ro-corcjozrlsfc.us-
east-1.docdb.amazonaws.com",
        "EnabledCloudwatchLogsExports": [
            "audit"
        ],
        "PreferredMaintenanceWindow": "wed:03:08-wed:03:38",
        "AssociatedRoles": [],
        "ClusterCreateTime": "2019-02-13T16:35:04.756Z",
        "DbClusterResourceId": "cluster-YOS52CUXGDTNKDQ7DH72I4LED4",
        "Endpoint": "sample-cluster.cluster-corcjozrlsfc.us-
east-1.docdb.amazonaws.com",
        "PreferredBackupWindow": "07:16-07:46",
        "DBClusterIdentifier": "sample-cluster"
    }
}
```

Deshabilitación de auditorías

Puede deshabilitar la auditoría deshabilitando la exportación de CloudWatch registros y deshabilitando el parámetro. `audit_logs`

Desactivar CloudWatch la exportación de registros

Puede deshabilitar la exportación de registros de auditoría mediante el Consola de administración de AWS o el AWS CLI.

Using the Consola de administración de AWS

El siguiente procedimiento utiliza el Consola de administración de AWS para deshabilitar la exportación de registros a Amazon DocumentDB. CloudWatch

Para deshabilitar los registros de auditoría

1. Inicie sesión en y abra la Consola de administración de AWS consola de Amazon DocumentDB en https://console.aws.amazon.com /docdb.
2. En el panel de navegación, seleccione Clusters (Clústeres). A continuación, elija el botón situado a la izquierda del nombre del clúster para el que desea deshabilitar la exportación de registros.
3. Elija Actions (Acciones) y después Modify (Modificar).

4. Desplácese hacia abajo hasta la sección Log exports (Exportaciones de registros) y, a continuación, elija Disabled (Deshabilitado).
5. Elija Continuar.
6. Revise los cambios y, a continuación, elija cuándo desea que se aplique este cambio en su clúster.

   - Apply during the next scheduled maintenance window (Aplicar durante el siguiente periodo de mantenimiento programado)
   - Apply immediately (Aplicar inmediatamente)
7. Elija Modificar clúster.

Using the AWS CLI

El siguiente código modifica el clúster `sample-cluster` e inhabilita los registros de auditoría. CloudWatch

Example

Para Linux, macOS o Unix:

```
aws docdb modify-db-cluster \
   --db-cluster-identifier sample-cluster \
   --cloudwatch-logs-export-configuration '{"DisableLogTypes":["audit"]}'
```

Para Windows:

```
aws docdb modify-db-cluster ^
   --db-cluster-identifier sample-cluster ^
   --cloudwatch-logs-export-configuration '{"DisableLogTypes":["audit"]}'
```

La salida de esta operación será similar a lo que se indica a continuación (formato JSON).

```
{
    "DBCluster": {
        "DBClusterParameterGroup": "default.docdb4.0",
        "HostedZoneId": "ZNKXH85TT8WVW",
        "MasterUsername": "<user-name>",
        "Status": "available",
        "Engine": "docdb",
        "Port": 27017,
```

```
        "AvailabilityZones": [
            "us-east-1a",
            "us-east-1c",
            "us-east-1f"
        ],
        "EarliestRestorableTime": "2019-02-13T16:35:50.387Z",
        "DBSubnetGroup": "default",
        "LatestRestorableTime": "2019-02-13T16:35:50.387Z",
        "DBClusterArn": "arn:aws:rds:us-east-1:900083794985:cluster:sample-
cluster2",
        "Endpoint": "sample-cluster2.cluster-corcjozrlsfc.us-
east-1.docdb.amazonaws.com",
        "ReaderEndpoint": "sample-cluster2.cluster-ro-corcjozrlsfc.us-
east-1.docdb.amazonaws.com",
        "BackupRetentionPeriod": 1,
        "EngineVersion": "4.0.0",
        "MultiAZ": false,
        "ClusterCreateTime": "2019-02-13T16:35:04.756Z",
        "DBClusterIdentifier": "sample-cluster2",
        "AssociatedRoles": [],
        "PreferredBackupWindow": "07:16-07:46",
        "DbClusterResourceId": "cluster-YOS52CUXGDTNKDQ7DH72I4LED4",
        "StorageEncrypted": false,
        "PreferredMaintenanceWindow": "wed:03:08-wed:03:38",
        "DBClusterMembers": [],
        "VpcSecurityGroups": [
            {
                "Status": "active",
                "VpcSecurityGroupId": "sg-77186e0d"
            }
        ]
    }
}
```

Deshabilitación del parámetro audit_logs

Para deshabilitar el parámetro `audit_logs` del clúster, puede modificar el clúster para que utilice un grupo de parámetros donde el valor del parámetro `audit_logs` esté `disabled`. O bien, puede modificar el valor del parámetro `audit_logs` en el grupo de parámetros del clúster para que esté `disabled`.

Para obtener más información, consulte los temas siguientes:

- Modificación de un clúster de Amazon DocumentDB
- Modificación de grupos de parámetros de clúster de Amazon DocumentDB

Acceso a los eventos de auditoría

Sigue los siguientes pasos para acceder a tus eventos de auditoría en Amazon CloudWatch.

1. Abre la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/.
2. Asegúrese de que se encuentra en la misma región que el clúster de Amazon DocumentDB.
3. En el panel de navegación, elija Logs (Registros).
4. Para buscar los registros de auditoría del clúster, busque y elija en la lista **`/aws/docdb/`*`yourClusterName`*`/audit`**.

   Los eventos de auditoría de cada una de las instancias están disponibles debajo del nombre de instancia correspondiente.

Filtrado de eventos de auditoría de DML

Introducción al filtrado de auditoría de DML

Los eventos de auditoría de DML se pueden filtrar antes de escribirlos en Amazon CloudWatch. Para utilizar esta característica, el registro de auditoría y el registro de DML deben estar habilitados. Amazon DocumentDB admite el filtrado en `atype`, `command`, `user`, `namespace` y `auditAuthorizationSuccess`.

> **Note**
>
> Los eventos DDL no se filtran.

Para habilitar el filtrado de auditoría en cualquier momento, especifique el filtro de auditoría mediante los parámetros `setAuditConfig`, `filter` y `auditAuthorizationSuccess` de la operación `db.adminCommand( { command } )`:

```
db.admin.runCommand(
   {
      setAuditConfig: 1,
```

```
      filter:
         {
            //filter conditions
         },
      auditAuthorizationSuccess: true | false
   }
)
```

También puede recuperar la configuración del filtro de auditoría mediante la ejecución del siguiente comando:

```
db.admin.runCommand( { getAuditConfig: 1})
```

Requisitos de seguridad

Solo las bases de datos users/roles con una acción privilegiada `auditConfigure` pueden ejecutar los comandos anteriores `admindb` al configurar o enumerar los filtros de auditoría de DML. Puede utilizar uno de los roles integrados de [`clusterAdmin`, `hostManager`, `root`] o crear roles personalizados con privilegios de `auditConfigure`. A continuación, se muestra un ejemplo del uso de los roles existentes con el privilegio de `auditConfigure` y un ejemplo con los roles personalizados.

Usuario con rol integrado:

```
use admin
db.createUser(
  {
    user: "myClusterAdmin",
    pwd: "password123",
    roles: [ { role: "clusterAdmin", db: "admin" } ]
  }
)
```

Usuario con roles personalizados:

```
use admin
db.createRole(
   {
     role: "myRole",
     privileges: [
       { resource: { cluster: true }, actions: [ "auditConfigure" ] }
```

```
     ],
     roles: []
   }
)
db.createUser(
  {
    user: "myUser",
    pwd: "myPassword",
    roles: [ { role: "myRole", db: "admin" } ]
  }
)
```

Filtrado de casos de uso

Ejemplo: filtrado de eventos por comandos

```
db.admin.runCommand(
   {
      setAuditConfig: 1,
      filter: {
        "$and": [
         {
            "param.command":
               {
                  $in: [ "find","count", "insert", "delete", "update",
 "findandmodify" ]
               }
         }
         ]
      },
      auditAuthorizationSuccess: true
   }
)
```

Ejemplo: filtrado de eventos por nombre de usuario

En este ejemplo, solo se registrará el usuario “myUser”:

```
db.admin.runCommand(
   {
      setAuditConfig: 1,
      filter: {
      "$and": [
```

```
         {
            "param.user":
               {
                  $in: [ "myUser" ]
               }
         }
         ]},
      auditAuthorizationSuccess: true})
```

Ejemplo: filtrado mediante **`atype`**

```
db.admin.runCommand(
   {
      setAuditConfig: 1,
      filter: {atype: "authCheck"},
      auditAuthorizationSuccess: true
   })
```

> **Note**
>
> Todos los registros de DML tienen `authCheck` como `atype`. Solo DDL tiene un `atype` diferente. Si coloca un valor que no sea el `authCheck` de`filter`, no se generará un inicio de sesión en DML. CloudWatch

Ejemplo: filtrado mediante varios filtros unidos por operadores

```
db.admin.runCommand(
   {
      setAuditConfig: 1,
      filter: {
      "$and": [
         {
            "param.command":
               {
                  $in: [ "find","count", "insert", "delete", "update",
 "findandmodify" ]
               }
         }
         ],
       "$nor": [
         {
```

```
            "param.command":
               {
                  $in: ["count", "insert", "delete", "update", "findandmodify" ]
               }
         }]
       },
      auditAuthorizationSuccess: true})
```

> **Note**
>
> En el nivel superior, solo se admiten `$and`, `$or` y `$nor`. Los demás operadores no se admiten y provocarán un error.

Ejemplo: filtrado mediante eventos por **`auditAuthorizationSuccess`**

En este filtro, no se registrarán todos los comandos que hayan pasado la autorización correctamente:

```
db.admin.runCommand(
   {
      setAuditConfig: 1,
      filter: {},
      auditAuthorizationSuccess: false
   }
)
```

Ejemplo: filtrado con condiciones **`$in`** y **`$nin`**

Si se utiliza `$in` y `$nin`, el comando no se registrará, ya que habrá un “y” implícito entre las condiciones. En este ejemplo, regex bloqueará el comando `find` para que no se registre nada:

```
db.admin.runCommand(
   {
      setAuditConfig: 1,
      filter: {
      "$and": [
         {
            atype: "authCheck",
            "param.command":
               {
                  $in: [ "find", "insert", "delete", "update", "findandmodify" ],
                  $nin: ["count", "insert", "delete", "update", "findandmodify" ],
```

```
                $not: /^^find.*/
            }
        },
        ],
       "$or": [
        {
           "param.command":
            {
               $nin: ["count", "insert", "delete", "update", "findandmodify" ]
            }
        }]
       },
      auditAuthorizationSuccess: true})
```

Ejemplo: filtrado mediante **`namespace`**

```
db.admin.runCommand(
   {
      setAuditConfig: 1,
      filter: {
      "$and": [
         {
            "param.ns":
               {
                  $in: [ "test.foo" ]
               }
         }
         ]},
      auditAuthorizationSuccess: true})
```

Ejemplo: restablecimiento del filtro predeterminado

Si se restablece el valor predeterminado, se registrarán todos los eventos de auditoría de DML. Para restablecer el filtrado al valor predeterminado, ejecute el siguiente comando:

```
db.admin.runCommand(
   {
      setAuditConfig: 1,
      filter: {},
      auditAuthorizationSuccess: true
   }
)
```

Amazon VPC y Amazon DocumentDB

Amazon Virtual Private Cloud (Amazon VPC) hace posible lanzar recursos de AWS, como instancias de Amazon DocumentDB, en una nube privada virtual (VPC).

Cuando utilice una VPC, puede controlar todos los aspectos del entorno de red virtual. Puede elegir su propio rango de direcciones IP, crear subredes y configurar listas de enrutamiento y control de acceso. Es posible ejecutar el clúster en una VPC sin costo adicional.

Las cuentas tienen una VPC predeterminada. Todos los clústeres nuevos se crean en la VPC predeterminada, a menos que se especifique lo contrario.

Temas

- Clústeres de DocumentDB en una VPC
- Acceso a un clúster de Amazon DocumentDB en una VPC
- Cree una VPC IPv4 exclusiva para usarla con un clúster de DocumentDB
- Creación de una VPC de pila doble para utilizarla con un clúster de DocumentDB

A continuación, encontrará una discusión acerca de la funcionalidad de la VPC relevante para los clústeres de Amazon DocumentDB. Para obtener más información sobre Amazon VPC, consulte la Guía del usuario de Amazon VPC.

Clústeres de DocumentDB en una VPC

Su clúster de Amazon DocumentDB es una nube privada virtual (VPC). Una VPC es una red virtual que está aislada lógicamente de otras redes virtuales del. Nube de AWS Amazon VPC le permite lanzar AWS recursos, como un clúster de Amazon DocumentDB o una instancia de Amazon, en una VPC. EC2 La VPC puede ser una VPC predeterminada que viene con la cuenta o una que se haya creado en ella. Todos VPCs están asociados a su cuenta. AWS

La VPC predeterminada tiene tres subredes que se pueden utilizar para aislar recursos dentro de la VPC. La VPC predeterminada también tiene una puerta de enlace de Internet que se puede utilizar para proporcionar acceso a los recursos situados dentro de la VPC desde fuera de la VPC.

Para ver las situaciones relacionadas con los clústeres de Amazon DocumentDB dentro y fuera de una VPC, consulte Acceso a un clúster de Amazon DocumentDB en una VPC.

Temas

- Trabajo con clústeres en una VPC
- Uso de grupos de subredes
- Direcciones IP de Amazon DocumentDB
- Creación de un clúster en una VPC

Trabajo con clústeres en una VPC

A continuación se ofrecen algunos consejos para trabajar con un clúster en una VPC:

- La VPC debe tener dos subredes como mínimo. Estas subredes deben estar en dos zonas de disponibilidad diferentes en la Región de AWS que desee implementar el clúster. Una subred es un segmento del rango de direcciones IP de una VPC que puede especificar y que le permite agrupar clústeres según sus necesidades operativas y de seguridad.
- Si desea que un clúster de la VPC sea accesible públicamente, asegúrese de activar los atributos `DNS hostnames` y `DNS resolution` de la VPC.
- La VPC debe tener un grupo de subredes que haya creado. Para crear un grupo de subredes, especifique las subredes que ha creado. Amazon DocumentDB elige una subred y una dirección IP dentro de esa subred para asociarla con la instancia principal de su clúster. La instancia principal utiliza la zona de disponibilidad que contiene la subred.
- La VPC debe tener un grupo de seguridad de VPC que permita el acceso al clúster.

  Para obtener más información, consulte Acceso a un clúster de Amazon DocumentDB en una VPC.
- Los bloques de CIDR de cada una de las subredes deben ser lo suficientemente grandes como para acomodar direcciones IP de repuesto para que Amazon DocumentDB las use durante las actividades de mantenimiento, incluyendo la conmutación por error y el escalado de recursos de computación. Por ejemplo, un rango como 10.0.0/24 y 10.0.2.0/24 suele ser lo suficientemente grande.
- Una VPC puede tener un atributo de `instance tenancy` de `default` o `dedicated`. Todos los valores predeterminados VPCs tienen el `instance tenancy` atributo establecido en default y una VPC predeterminada puede admitir cualquier clase de instancia.

  Si eliges tener tu clúster en una VPC dedicada en la que el `instance tenancy` atributo esté establecido`dedicated`, la clase de instancia del clúster debe ser uno de los tipos de instancias EC2 dedicadas aprobados por Amazon. Por ejemplo, la instancia `r5.large` EC2 dedicada corresponde a la clase de `db.r5.large` instancia. Para obtener información sobre el

arrendamiento de instancias en una VPC, consulte Amazon instances en la EC2 Guía del usuario de Amazon Elastic Compute Cloud.

Para obtener más información sobre los tipos de instancias que pueden estar en una instancia dedicada, consulta Instancias EC2 dedicadas de Amazon en la página de EC2 precios de Amazon.

> **Note**
>
> Cuando establece el atributo de `instance tenancy` en `dedicated` para un clúster, no garantiza que el clúster se ejecute en un host dedicado.

Uso de grupos de subredes

Las subredes son segmentos del rango de direcciones IP de una VPC que se definen para agrupar recursos de acuerdo con las necesidades operativas y de seguridad. Los grupos de subredes son una colección de subredes (normalmente privadas) que crea en una VPC y que después asigna a los clústeres. Al utilizar un grupo de subredes, puede especificar una VPC concreta al crear clústeres mediante AWS CLI la API o Amazon DocumentDB. Si utiliza la consola, solo puede elegir la VPC y los grupos de subredes que desea utilizar.

Cada grupo de subredes debe tener subredes como mínimo en dos zonas de disponibilidad de una Región de AWS determinada. Cuando crea un clúster en una VPC, debe elegir un grupo de subredes. Del grupo de subredes, Amazon DocumentDB elige una subred y una dirección IP dentro de esa subred para asociarla con la instancia principal de su clúster. La base de datos utiliza la zona de disponibilidad que contiene la subred. DocumentDB siempre asigna una dirección IP desde una subred que tiene espacio de dirección IP libre.

Las subredes de un grupo de subredes son públicas o privadas, según la configuración que haya establecido para sus listas de control de acceso a la red (red ACLs) y tablas de enrutamiento. Para que un clúster sea accesible públicamente, todas las subredes del grupo de subredes deben ser públicas. Si una subred asociada a un clúster de acceso público cambia de pública a privada, eso puede afectar la disponibilidad del clúster.

Para crear un grupo de subredes que admita el modo de doble pila, asegúrese de que cada subred que agregue al grupo de subredes tenga asociado un bloque CIDR del Protocolo de Internet versión 6 (IPv6). Para obtener más información, consulte la Guía del usuario de Amazon Virtual Private Cloud Direcciones IP de Amazon DocumentDB y el IPv6 soporte para su VPC.

Cuando Amazon DocumentDB crea un clúster en una VPC, asigna una interfaz de red al clúster con la dirección IP seleccionada del grupo de subredes. Sin embargo, le recomendamos que utilice el nombre del sistema de nombres de dominio (DNS) para conectarse al clúster. Se recomienda hacerlo porque la dirección IP subyacente cambia durante la conmutación por error.

> **Note**
>
> Para cada clúster que ejecute en una VPC, asegúrese de reservar al menos una dirección en cada subred del grupo de subredes para que la utilice Amazon DocumentDB para las acciones de recuperación.

Subredes compartidas

Puede crear un clúster en una VPC compartida.

Algunas consideraciones que se deben tener en cuenta al utilizar la versión compartida VPCs:

- Puede mover un clúster de una subred de VPC compartida a una subred de VPC no compartida y viceversa.
- Los participantes de una VPC compartida deben crear un grupo de seguridad en la VPC que les permita crear un clúster.
- Los propietarios y los participantes de una VPC compartida pueden acceder a la base de datos mediante consultas en DocumentDB. Sin embargo, solo el creador de un recurso puede realizar llamadas a la API en el recurso.

Direcciones IP de Amazon DocumentDB

Las direcciones IP permiten que los recursos de la VPC se comuniquen entre sí y con otros recursos a través de Internet. Amazon DocumentDB admite ambos IPv4 protocolos de IPv6 direccionamiento. De forma predeterminada, Amazon DocumentDB y Amazon VPC utilizan el protocolo de direccionamiento. IPv4 No puedes desactivar este comportamiento. Al crear una VPC, asegúrese de especificar un bloque IPv4 CIDR (un rango de direcciones privadas IPv4). Si lo desea, puede asignar un bloque IPv6 CIDR a la VPC y las subredes, y IPv6 asignar las direcciones de ese bloque a los clústeres de la subred.

> **Note**
>
> El modo de doble pila (IPv6 direccionamiento) solo se admite en las versiones 4.0 y 5.0 de Amazon DocumentDB.

Support for the IPv6 protocol amplía el número de direcciones IP compatibles. Al utilizar el IPv6 protocolo, se asegura de tener suficientes direcciones disponibles para el futuro crecimiento de Internet. Los recursos y IPv6 direcciones de DocumentDB nuevos IPv4 y existentes se pueden utilizar dentro de su VPC. Configurar, proteger y traducir el tráfico de red entre los dos protocolos utilizados en diferentes partes de una aplicación puede provocar sobrecarga operativa. Puede estandarizar el IPv6 protocolo de los recursos de Amazon DocumentDB para simplificar la configuración de la red.

Temas

- IPv4 direcciones
- IPv6 direcciones
- Modo de pila doble

IPv4 direcciones

Al crear una VPC, debe especificar un rango de IPv4 direcciones para la VPC en forma de bloque CIDR, por ejemplo. `10.0.0.0/16` Un grupo de subredes define el rango de direcciones IP de este bloque de CIDR que puede utilizar un clúster. Esta dirección IP puede ser privada o pública.

Una IPv4 dirección privada es una dirección IP a la que no se puede acceder a través de Internet. Puedes usar IPv4 direcciones privadas para la comunicación entre tu clúster y otros recursos, como las EC2 instancias de Amazon, en la misma VPC. Cada clúster tiene una dirección IP privada para la comunicación en la VPC.

Una dirección IP pública es una IPv4 dirección a la que se puede acceder desde Internet. No se permiten las direcciones IP públicas en el clúster de DocumentDB. Cualquier dirección IP pública debe resolverse en la puerta de enlace de Internet y EC2 en la subred pública.

Para ver cómo crear una VPC solo con IPv4 direcciones privadas que pueda usar en un escenario común de Amazon DocumentDB, consulte. Cree una VPC IPv4 exclusiva para usarla con un clúster de DocumentDB

IPv6 direcciones

Si lo desea, puede asociar un bloque IPv6 CIDR a su VPC y sus subredes, y IPv6 asignar direcciones de ese bloque a los recursos de su VPC. Cada IPv6 dirección es única a nivel mundial.

El bloque IPv6 CIDR de su VPC se asigna automáticamente desde el conjunto IPv6 de direcciones de Amazon. Usted no puede elegir el rango.

Al conectarse a una IPv6 dirección, asegúrese de que se cumplen las siguientes condiciones:

- El cliente está configurado de modo que se permita el paso IPv6 del tráfico del cliente a la base de datos.
- Los grupos de seguridad de DocumentDB utilizados por el clúster están configurados correctamente para permitir el cruce del tráfico del cliente a la base de IPv6 datos.
- La pila de sistemas operativos del cliente permite el tráfico en la IPv6 dirección, y los controladores y bibliotecas del sistema operativo están configurados para elegir el punto final del clúster predeterminado correcto (uno IPv4 o varios IPv6).

Para obtener más información IPv6, consulte Direcciones IP en la Guía del usuario de Amazon Virtual Private Cloud.

Modo de pila doble

Cuando un clúster puede comunicarse a través del protocolo de IPv6 direccionamiento IPv4 y el protocolo de direccionamiento, se ejecuta en modo de doble pila. Por lo tanto, los recursos pueden comunicarse con el clúster a través IPv4 de o ambos. IPv6 DocumentDB deshabilita el acceso a Internet Gateway para los IPv6 puntos finales de los clústeres privados en modo de doble pila. DocumentDB lo hace para garantizar que sus IPv6 puntos de conexión sean privados y solo se pueda acceder a ellos desde su VPC.

Temas

- Modo de pila doble y grupos de subredes
- Trabajo con clústeres en modo de pila doble
- Modificación IPv4 de clústeres exclusivos para utilizar el modo de doble pila
- Disponibilidad del modo de pila doble según la región y versión
- Limitaciones de los clústeres de red de pila doble

Modo de pila doble y grupos de subredes

Para usar el modo de doble pila, asegúrese de que cada subred del grupo de subredes que asocie al clúster tenga un IPv6 bloque CIDR asociado. Puede crear un nuevo grupo de subredes o modificar un grupo existente de subredes para cumplir este requisito. Cuando un clúster esté en modo de pila doble, los clientes podrán conectarse como siempre. Asegúrese de que los firewalls de seguridad del cliente y los grupos de seguridad del clúster de DocumentDB estén configurados correctamente para permitir el paso del tráfico. IPv6 Para conectarse, los clientes utilizan el punto de conexión del clúster. Las aplicaciones de cliente pueden especificar qué protocolo prefieren al conectarse a una base de datos. En el modo de doble pila, el clúster detecta el protocolo de red preferido del cliente, ya sea IPv4 o no IPv6, y lo utiliza para la conexión.

Si un grupo de subredes deja de admitir el modo de pila doble debido a la eliminación de subredes o a la disociación de CIDR, existe el riesgo de que se produzca un estado de red incompatible para los clústeres asociados al grupo de subredes. Además, no puede utilizar el grupo de subredes cuando crea un clúster nuevo en modo de pila doble.

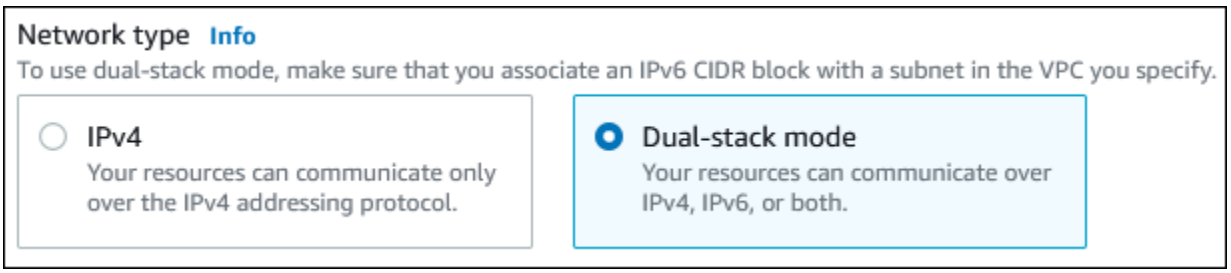
Para determinar si un grupo de subredes admite el modo de doble pila mediante el Consola de administración de AWS, consulte el tipo de red en la página de detalles del grupo de subredes. Para determinar si un grupo de subredes admite el modo de doble pila mediante el AWS CLI, ejecute el `describe-db-subnet-groups`comando y visualícelo en el resultado. `SupportedNetworkTypes`

Las réplicas de lectura se tratan como clústeres independientes y pueden tener un tipo de red diferente al del clúster principal. Si cambia el tipo de red del clúster principal de una réplica de lectura, la réplica de lectura no se verá afectada. Cuando restaura un clúster, puede restaurarla a cualquier tipo de red compatible.

Trabajo con clústeres en modo de pila doble

Al crear o modificar un clúster, puede especificar el modo de doble pila para permitir que los recursos se comuniquen con el clúster a través IPv4 de él o de ambos modos. IPv6

Al utilizar el Consola de administración de AWS para crear o modificar un clúster, puede especificar el modo de doble pila en la sección Tipo de red. En la imagen siguiente se muestra la sección Tipo de red en la consola:



Cuando utilice el AWS CLI para crear o modificar un clúster, defina la `--network-type` opción `DUAL` para utilizar el modo de doble pila. Si utiliza la API de DocumentDB para crear o modificar un clúster, establezca el parámetro `NetworkType` en `DUAL` para utilizar el modo de pila doble. Si el modo de pila doble no es compatible con la versión del motor ni el grupo de subredes de DocumentDB especificados, se devuelve el error `NetworkTypeNotSupported`.

Para obtener más información acerca de la creación de un clúster, consulte Creación de un clúster de Amazon DocumentDB. Para obtener más información sobre la modificación de un clúster, consulteModificación de un clúster de Amazon DocumentDB.

Para determinar si un clúster está en modo de pila doble mediante la consola, consulte Tipo de red en la pestaña Conectividad y seguridad del clúster.

Modificación IPv4 de clústeres exclusivos para utilizar el modo de doble pila

Puede modificar un clúster IPv4 exclusivo para usar el modo de doble pila. Para ello, cambie el tipo de red del clúster.

Se recomienda cambiar el tipo de red del clúster de Amazon DocumentDB durante un período de mantenimiento. Puede configurar el tipo de red manualmente mediante el comando `modify-db-cluster`.

Antes de modificar un clúster para utilizar el modo de pila doble, asegúrese de que su grupo de subredes admite el modo de pila doble. Si el grupo de subredes asociado al clúster no admite el modo de pila doble, especifique otro grupo de subredes que lo admita cuando modifique el clúster. La modificación del grupo de subredes de un clúster puede provocar un tiempo de inactividad.

Si modifica el grupo de subredes de un clúster antes de cambiar el clúster para utilizar el modo de pila doble, asegúrese de que el grupo de subredes sea válido para el clúster antes del cambio y después de este.

Le recomendamos que ejecute la llamada `ModifyDBCluster` solo con el parámetro `NetworkType` establecido en `DUAL` para cambiar la red al modo de pila doble. Si se añaden otros parámetros junto

con `NetworkType` en la misma llamada a la API, se podría producir un tiempo de inactividad. Para modificar varios parámetros, asegúrese de que la modificación del tipo de red se haya completado correctamente antes de enviar otra solicitud de `ModifyDBCluster` con otros parámetros.

Si no puede conectarse al clúster después del cambio, asegúrese de que los firewalls de seguridad del cliente y de la base de datos y las tablas de enrutamiento estén configurados correctamente para permitir el tráfico a la base de datos en la red seleccionada (o bien IPv4). IPv6 Es posible que también necesite modificar los parámetros, las bibliotecas o los controladores del sistema operativo para conectarse mediante una IPv6 dirección.

Para modificar un clúster IPv4 exclusivo para usar el modo de doble pila

1. Modifique un grupo de subredes para admitir el modo de pila doble o cree un grupo de subredes que admita el modo de pila doble:

   a. Asocie un bloque IPv6 CIDR a su VPC.

      Para obtener las instrucciones, consulte Adición o eliminación de un bloque de CIDR de su VPC en la Guía del usuario de Amazon VPC.

   b. Adjunte el bloque IPv6 CIDR a todas las subredes de su grupo de subredes.

      Para obtener instrucciones, consulte Añadir o eliminar un bloque IPv6 CIDR a su subred en la Guía del usuario de Amazon Virtual Private Cloud.

   c. Confirme que el grupo de subredes admita el modo de pila doble.

      Si está utilizando el Consola de administración de AWS, seleccione el grupo de subredes y asegúrese de que el valor Tipos de red compatibles sea Doble.

      Si está utilizando el AWS CLI, ejecute el `describe-db-subnet-groups`comando y asegúrese de que el `SupportedNetworkType` valor del clúster sea`Dual`.

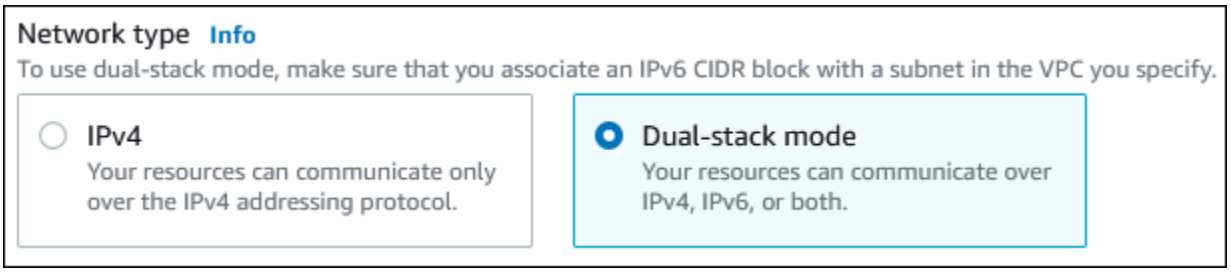
2. Modifique el grupo de seguridad asociado al clúster para permitir IPv6 las conexiones a la base de datos o cree un nuevo grupo de seguridad que permita IPv6 las conexiones.

   Para obtener más información, consulte Reglas del grupo de seguridad en la Guía del usuario de Amazon Virtual Private Cloud.

3. Modifique el clúster para admitir el modo de pila doble. Para ello, defina Network type (Tipo de red) en Dual-stack mode (Modo de pila doble).

   Si utiliza la consola, asegúrese de que la siguiente configuración sea correcta:

- Tipo de red: modo de pila doble



- Grupo de subredes: el grupo de subredes que configuró en un paso anterior.
- Grupo de seguridad: la seguridad que configuró en el paso anterior.

Si está utilizando el AWS CLI, asegúrese de que la siguiente configuración sea correcta:

- `--network-type` — `dual`
- `--db-subnet-group-name`: el grupo de subredes que configuró en un paso anterior.
- `--vpc-security-group-ids`: el grupo de seguridad de la VPC que configuró en un paso anterior.

Por ejemplo:

```
aws docdb modify-db-cluster --db-cluster-identifier <cluster-name> --network-type
 "DUAL"
```

4. Confirme que el clúster admite el modo de pila doble.

   Si utiliza la consola, elija la pestaña Conectividad y seguridad del clúster y asegúrese de que el valor de Tipo de red sea Modo de pila doble.

   Si está utilizando el AWS CLI, ejecute el `describe-db-cluster` comando y asegúrese de que el `NetworkType` valor del clúster es`dual`.

   Ejecute el `dig` comando en el punto final del clúster para identificar la IPv6 dirección asociada a él:

   ```
   dig <db-cluster-endpoint> AAAA
   ```

   Utilice el punto final del clúster, no la IPv6 dirección, para conectarse al clúster.

Disponibilidad del modo de pila doble según la región y versión

La disponibilidad y la compatibilidad de las características varían en las Regiones de AWS.

Compatibilidad de regiones

La siguiente lista identifica los Regiones de AWS que admiten el modo de doble pila:

- Este de EE. UU. (Ohio)
- Este de EE. UU. (Norte de Virginia)
- Oeste de EE. UU. (Oregón)
- África (Ciudad del Cabo)
- América del Sur (São Paulo)
- Asia-Pacífico (Hong Kong)
- Asia-Pacífico (Hyderabad)
- Asia-Pacífico (Malasia)
- Asia-Pacífico (Mumbai)
- Asia-Pacífico (Osaka)
- Asia-Pacífico (Seúl)
- Asia-Pacífico (Singapur)
- Asia-Pacífico (Sídney)
- Asia-Pacífico (Yakarta)
- Asia-Pacífico (Tailandia)
- Asia-Pacífico (Tokio)
- Canadá (centro)
- China (Pekín)
- China (Ningxia)
- Europa (Fráncfort)
- Europa (Irlanda)
- Europa (Londres)
- Europa (Milán)
- Europa (París)
- Europa (España)

- Europa (Estocolmo)
- Israel (Tel Aviv)
- México (centro)
- Medio Oriente (EAU)
- AWS GovCloud (EE. UU.-Oeste)
- AWS GovCloud (Estados Unidos-Este)

Soporte de versiones

Las versiones 4.0 y 5.0 de Amazon DocumentDB son compatibles con el modo de pila doble. Si no puede acceder al modo de pila doble en ninguna de estas versiones, asegúrese de que está ejecutando la última versión del parche del motor en su clúster.

Limitaciones de los clústeres de red de pila doble

Las siguientes limitaciones se aplican a los clústeres de red de pila doble:

- Los clústeres no pueden utilizar el IPv6 protocolo de forma exclusiva. Pueden usarlo IPv4 exclusivamente o pueden usar el IPv6 protocolo IPv4 and (modo de doble pila).
- Amazon DocumentDB no admite subredes nativas IPv6 .
- Los clústeres que utilizan el modo de pila doble deben ser de tipo privado. No pueden ser accesibles públicamente.

Creación de un clúster en una VPC

Los siguientes procedimientos le permiten crear un clúster en una VPC. Para utilizar la VPC predeterminada, puede comenzar con el paso 2 y utilizar la VPC y el grupo de subredes que ya se han creado para usted. También puede crear más VPCs, si es necesario.

> **Note**
>
> Si desea que el clúster de la VPC sea accesible públicamente, debe actualizar la información de DNS para la VPC. Para ello, active los atributos `DNS hostnames` y `DNS resolution` de la VPC. Para obtener más información sobre la actualización del DNS de una instancia de VPC, consulte Ver y actualizar los atributos de DNS de su VPC en la Guía del usuario de Amazon Virtual Private Cloud.

Para crear un clúster en una VPC, siga estos pasos:

- Paso 1: Crear una VPC
- Paso 2: crear un grupo de subredes
- Paso 3: Crear un grupo de seguridad de VPC
- Paso 4: crear un clúster en la VPC

Paso 1: Crear una VPC

Cree una VPC con subredes en al menos dos zonas de disponibilidad. Utilizará estas subredes cuando cree un grupo de subredes. Si tiene una VPC predeterminada, se crea automáticamente una subred en cada zona de disponibilidad de la Región de AWS.

Para obtener más información, consulte Cree una VPC IPv4 exclusiva para usarla con un clúster de DocumentDB o consulte Creación de una VPC en la Guía del usuario de Amazon Virtual Private Cloud.

Paso 2: crear un grupo de subredes

Los grupos de subredes son una colección de subredes (normalmente privadas) que crea para una VPC y que después asigna a los clústeres. Un grupo de subredes le permite especificar una VPC concreta al crear clústeres mediante la API AWS CLI o la API de DocumentDB. Si usas la Consola de administración de AWS, solo tienes que elegir la VPC y las subredes que quieres usar. Cada grupo de subredes debe tener como mínimo una subred en, al menos, dos zonas de disponibilidad de la Región de AWS. Como práctica recomendada, cada grupo de subredes debería tener al menos una subred por cada una de las zonas de disponibilidad en la Región de AWS.

Para que un clúster sea accesible públicamente, las subredes del grupo de subredes deben tener una puerta de enlace de Internet. Para obtener más información sobre las puertas de enlace de Internet para las subredes, consulte Activación del acceso a Internet de una VPC con una puerta de enlace de Internet en la Guía del usuario de Amazon Virtual Private Cloud.

> **Note**
>
> El grupo de subredes para una zona local puede tener solo una subred.

Cuando crea un clúster en una VPC, puede elegir un grupo de subredes. Amazon DocumentDB elige una subred y una dirección IP (dentro de esa subred) para asociarla con el clúster. Si no existen

grupos de subredes, Amazon DocumentDB crea un grupo de subredes predeterminado cuando crea el clúster. DocumentDB crea y asocia una interfaz de red elástica a su clúster con esa dirección IP. El clúster utiliza la zona de disponibilidad que contiene la subred.

En este paso, debe crear un grupo de subredes y debe agregar las subredes que creó para la VPC.

Para crear un grupo de subredes

1. Inicie sesión en y abra la Consola de administración de AWS consola de Amazon DocumentDB en https://console.aws.amazon.com /docdb.
2. En el panel de navegación, elija Subnet groups (grupos de subredes).
3. Seleccione Crear.
4. En Nombre, escriba el nombre del grupo de subredes.
5. En Descripción, escriba la descripción del grupo de subredes.
6. En la sección Añadir subredes, para VPC, elija la VPC predeterminada o la VPC que creó. A continuación, elija las zonas de disponibilidad que incluyen las subredes en Zonas de disponibilidad, y, luego, elija las subredes en Subredes.
7. Seleccione Crear.

   El nuevo grupo de subredes aparece en la lista de Grupos de subredes de la consola de DocumentDB. Puede elegir el grupo de subredes para ver los detalles, incluidas todas las subredes asociadas al grupo, en el panel de detalles de la parte inferior de la ventana.

Paso 3: Crear un grupo de seguridad de VPC

Antes de crear el clúster, cree un grupo de seguridad de la VPC para asociarlo a él. Si no crea un grupo de seguridad de VPC, puede utilizar el grupo de seguridad predeterminado cuando cree el clúster. Para obtener instrucciones sobre cómo crear un grupo de seguridad para su clústerCree una VPC IPv4 exclusiva para usarla con un clúster de DocumentDB, consulte o consulte Controlar el tráfico de sus AWS recursos mediante grupos de seguridad en la Guía del usuario de Amazon Virtual Private Cloud.

Paso 4: crear un clúster en la VPC

En este paso, se crea un clúster con el nombre de la VPC, el grupo de subredes y el grupo de seguridad de la VPC que creó en los pasos anteriores.

> **Note**
>
> Si desea que un clúster de la VPC sea accesible públicamente, debe activar los atributos `DNS hostnames` y `DNS resolution` de la VPC. Para obtener más información, consulte Ver y actualizar los atributos de DNS de su VPC en la Guía del usuario de Amazon Virtual Private Cloud.

Para obtener información detallada acerca de cómo crear un clúster, consulte Creación de un clúster de Amazon DocumentDB.

Cuando la sección Conectividad se lo pida, introduzca el nombre de la VPC, el grupo de subredes y el grupo de seguridad de la VPC.

> **Note**
>
> Actualmente, los clústeres de DBDocument bases de datos de documentos VPCs no admiten la actualización.

Acceso a un clúster de Amazon DocumentDB en una VPC

Amazon DocumentDB admite las siguientes situaciones para obtener acceso a un clúster en una VPC:

Temas

- Un clúster de una VPC al que accede una EC2 instancia de Amazon en la misma VPC
- Un clúster de una VPC al que accede una EC2 instancia de Amazon en una VPC diferente

Un clúster de una VPC al que accede una EC2 instancia de Amazon en la misma VPC

Un uso común de un clúster en una VPC es compartir datos con un servidor de aplicaciones que se ejecuta en una EC2 instancia de Amazon en la misma VPC.

La forma más sencilla de administrar el acceso entre EC2 instancias y clústeres en la misma VPC es hacer lo siguiente:

- Cree un grupo de seguridad de VPC para sus clústeres. Este grupo de seguridad se puede utilizar para restringir el acceso a los clústeres. Por ejemplo, puede crear una regla personalizada para este grupo de seguridad. Esto puede permitir el acceso TCP mediante el uso del puerto que asignó al clúster cuando lo creó y una dirección IP que utiliza para acceder al clúster para el desarrollo u otras finalidades.
- Cree un grupo de seguridad de VPC en el que estén sus EC2 instancias (servidores web y clientes). Si es necesario, este grupo de seguridad puede permitir el acceso a la EC2 instancia desde Internet mediante la tabla de enrutamiento de la VPC. Por ejemplo, puedes establecer reglas en este grupo de seguridad para permitir el acceso TCP a la EC2 instancia a través del puerto 22.
- Crea reglas personalizadas en el grupo de seguridad para tus clústeres que permitan las conexiones desde el grupo de seguridad que creaste para tus EC2 instancias. Estas reglas podrían permitir que cualquier miembro del grupo de seguridad acceda a los clústeres.

Hay una subred pública y privada adicional en una zona de disponibilidad independiente. Los grupos de subredes de DocumentDB requieren una subred en, al menos, dos zonas de disponibilidad. La subred adicional facilita el cambio a una implementación de clúster multi-AZ en el futuro.

Para conocer las instrucciones sobre cómo crear una VPC con subredes públicas y privadas para esta situación, consulte Cree una VPC IPv4 exclusiva para usarla con un clúster de DocumentDB.

> **Tip**
>
> Puede configurar automáticamente la conectividad de red entre una EC2 instancia de Amazon y un clúster de DocumentDB al crear el clúster. Para obtener más información, consulte Connect Amazon EC2 automáticamente.

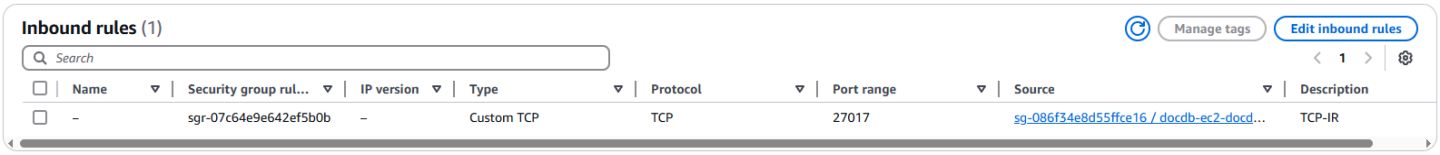
Para crear una regla en un grupo de seguridad de VPC que permita las conexiones desde otro grupo de seguridad, haga lo siguiente:

1. Inicie sesión en la consola de Amazon VPC Consola de administración de AWS y ábrala en https://console.aws.amazon.com /vpc.
2. En el panel de navegación, ubique y elija Grupos de seguridad.
3. Elija o cree el grupo de seguridad al que desea que puedan tener acceso los miembros de otro grupo de seguridad. Este es el grupo de seguridad que usa para los clústeres. Elija la pestaña

Inbound Rules (Reglas de entrada) y, a continuación, elija Edit inbound rules (Editar reglas de entrada).

4. En la página Edit inbound rules (Editar reglas de entrada), elija Add Rule (Agregar regla).
5. En Tipo, elija la entrada que corresponda al puerto que utilizó cuando creó el clúster, como TCP personalizada.
6. En el campo Origen, comience a escribir el identificador del grupo de seguridad, que enumera los grupos de seguridad coincidentes. Elija el grupo de seguridad cuyos miembros desea que tengan acceso a los recursos protegidos por este grupo de seguridad. En el escenario anterior, este es el grupo de seguridad que se utiliza para la instancia. EC2
7. Si es necesario, repita los pasos para el protocolo TCP y cree una regla con Todo TCP como Tipo y el grupo de seguridad en el campo Origen. Si va a utilizar el protocolo UDP, cree una regla con All UDP (Todo UDP) en el campo Type (Tipo) y con el grupo de seguridad en el campo Source (Origen).
8. Seleccione Guardar reglas.

La siguiente pantalla muestra una regla de entrada con un grupo de seguridad para su origen.



Para obtener más información sobre cómo conectarse a un clúster desde la EC2 instancia, consulteConnect Amazon EC2 automáticamente.

Un clúster de una VPC al que accede una EC2 instancia de Amazon en una VPC diferente

Si los clústeres se encuentran en una VPC diferente de la EC2 instancia que está utilizando para acceder a ellos, puede utilizar la interconexión de VPC para acceder al clúster.

Una conexión de emparejamiento de VPC es una conexión de red entre dos VPCs que le permite enrutar el tráfico entre ellas mediante direcciones IP privadas. Los recursos de ambas VPC se pueden comunicar entre sí siempre que se encuentren en la misma red. Puedes crear una conexión de emparejamiento de VPC entre la tuya VPCs, con una VPC de otra AWS cuenta o con una VPC de otra. Región de AWS Para obtener más información sobre las interconexiones de VPC, consulte Interconexión con VPC en la Guía de usuario de Amazon Virtual Private Cloud.

Cree una VPC IPv4 exclusiva para usarla con un clúster de DocumentDB

Una situación común incluye un clúster en una nube privada virtual (VPC) basada en el servicio Amazon VPC. Por ejemplo, esta VPC podría compartir datos con un servicio o aplicación que se ejecute en la misma VPC. En este tema, creará la VPC para esta situación.

Temas

- Paso 1: crear una VPC con subredes públicas y privadas
- Paso 2: crear un grupo de seguridad de VPC para una aplicación pública
- Paso 3: crear un grupo de seguridad de VPC para un clúster privado
- Paso 4: Crear un grupo de subredes
- Eliminación de una VPC

Su clúster debe estar disponible únicamente para su servidor web, y no para la Internet pública. Además, cree de una VPC con subredes públicas y privadas. La aplicación se aloja en la subred pública, para que pueda obtener acceso a la Internet pública. El clúster se aloja en una subred privada. La aplicación puede conectarse al clúster porque se aloja en la misma VPC. Sin embargo, el clúster no está disponible en la red pública de internet, lo que proporciona mayor seguridad.

Con el procedimiento de este tema se configura una subred pública y privada adicional en una zona de disponibilidad independiente. El procedimiento no utiliza estas subredes. Los grupos de subredes de DocumentDB requieren una subred en, al menos, dos zonas de disponibilidad. La subred adicional facilita la configuración de más de una instancia de DocumentDB.

En este tema se describe la configuración de una VPC para clústeres de Amazon DocumentDB. Para obtener más información sobre Amazon VPC, consulte la Guía del usuario de Amazon VPC.

> **Tip**
>
> Puede configurar automáticamente la conectividad de red entre una EC2 instancia de Amazon y un clúster de DocumentDB al crear el clúster. La configuración de red es similar a la que se describe en esta situación. Para obtener más información, consulte Connect Amazon EC2 automáticamente.

Paso 1: crear una VPC con subredes públicas y privadas

Utilice el siguiente procedimiento para crear una VPC con subredes públicas y privadas.

Para crear una VPC y subredes

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com /vpc.
2. En la esquina superior derecha de Consola de administración de AWS, elige la región en la que quieres crear tu VPC. En este ejemplo se utiliza la región Oeste de EE. UU. (Oregón).
3. En la esquina superior izquierda, elija VPC Dashboard (Panel de control VPC). Para comenzar a crear una VPC, elija Create VPC (Crear una VPC).
4. En Resources to create (Recursos para crear), en VPC settings (Configuración VPC), elija VPC and more (VPC y más).
5. En VPC settings (Configuración de la VPC), establezca estos valores:
   - Generación automática de etiquetas de identificación — **`example`**
   - IPv4 Bloque CIDR — **`10.0.0.0/16`**
   - IPv6 Bloque CIDR: sin IPv6 bloqueo CIDR
   - Tenencia: predeterminada
   - Número de zonas de disponibilidad (AZs): 2
   - Personalizar AZs: mantenga los valores predeterminados
   - Número de subredes públicas: 2
   - Número de subredes privadas: 2
   - Personalizar bloques de CIDR de subredes: conserve los valores predeterminados.
   - Puertas de enlace NAT ($): ninguna
   - Puntos de conexión de VPC: ninguno
   - Opciones de DNS: conserve los valores predeterminados.
6. Seleccione Creación de VPC.

Paso 2: crear un grupo de seguridad de VPC para una aplicación pública

A continuación, cree un grupo de seguridad para el acceso público. Para conectarse a las EC2 instancias públicas de la VPC, debe agregar reglas de entrada al grupo de seguridad de la VPC. Permiten que el tráfico se conecte desde Internet.

Para crear un grupo de seguridad de VPC

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com /vpc.
2. Elija VPC Dashboard (Panel VPC), seguido de Security Groups (Grupos de seguridad) y, por último, Create Security Group (Crear grupo de seguridad).
3. En la página Create Security Group (Crear grupo de seguridad), establezca estos valores:
   - Nombre del grupo de seguridad: **`example-securitygroup`**
   - Descripción — **`Application security group`**
   - VPC: elija la VPC que creó anteriormente, por ejemplo: vpc-example.
4. Agregar reglas de entrada al grupo de seguridad
   a. Determine la dirección IP que se utilizará para conectarse a EC2 las instancias de la VPC mediante Secure Shell (SSH). Para determinar su dirección IP pública, en otra ventana o pestaña del navegador, puede utilizar el servicio en. https://checkip.amazonaws.com Un ejemplo de dirección IP es `203.0.113.25/32`.

      En muchos casos, puede conectarse a través de un proveedor de servicios de internet (ISP) o protegido por un firewall sin una dirección IP estática. Si es así, busque el rango de direcciones IP utilizadas por los ordenadores cliente.

      > ⚠ Warning
      >
      > Si utiliza `0.0.0.0/0` para el acceso SSH, permita que todas las direcciones IP accedan a sus instancias públicas mediante SSH. Este método es aceptable para un periodo de tiempo corto en un entorno de prueba, pero no es seguro en entornos de producción. En entornos de producción, solo debe autorizar una dirección IP específica o un intervalo de direcciones para acceder a sus instancias mediante SSH.

   b. En la sección Inbound rules (Reglas de entrada), elija Add rule (agregar regla).
   c. Establece los siguientes valores para tu nueva regla de entrada para permitir el acceso de SSH a tu instancia de Amazon EC2 . Una vez hecho esto, puedes conectarte a tu EC2 instancia para instalar la aplicación y otras utilidades. También te conectas a tu EC2 instancia para cargar contenido para tu aplicación.
      - Escriba — **`SSH`**

- Origen: la dirección IP o el rango de direcciones que creó en el Paso a, por ejemplo: **`203.0.113.25/32`**.

d. Seleccione Agregar regla.

e. Establezca los siguientes valores para la regla de entrada nueva con objeto de permitir el acceso HTTP a su aplicación.

- Tipo — **`HTTP`**
- Fuente — **`0.0.0.0/0`**

5. Para crear el grupo de seguridad, elija Create security group (Crear grupo de seguridad).

   Anote el identificador del grupo de seguridad, ya que lo necesitará más tarde en otro procedimiento.

Paso 3: crear un grupo de seguridad de VPC para un clúster privado

Para crear un clúster privado, debe crear un segundo grupo de seguridad para el acceso privado. Para conectarse a clústeres privados en la VPC, agregue reglas de entrada al grupo de seguridad de la VPC que permitan el tráfico solo desde su aplicación.

Para crear un grupo de seguridad de VPC

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com /vpc.
2. Elija VPC Dashboard (Panel VPC), seguido de Security Groups (Grupos de seguridad) y, por último, Create Security Group (Crear grupo de seguridad).
3. En la página Create Security Group (Crear grupo de seguridad), establezca estos valores:
   - Nombre del grupo de seguridad: **`example-securitygroup`**
   - Descripción — **`Instance security group`**
   - VPC: elija la VPC que creó anteriormente, por ejemplo: vpc-example.
4. Agregar reglas de entrada al grupo de seguridad

   a. En la sección Inbound rules (Reglas de entrada), elija Add rule (gregar regla).

   b. Defina los siguientes valores para la nueva regla de entrada a fin de permitir el tráfico de DocumentDB en el puerto 27017 desde su instancia de Amazon. EC2 Si lo hace, podrá conectarse desde su aplicación a su clúster. Si lo hace, puede almacenar y recuperar datos desde su aplicación a su base de datos.

- Escriba: **`Custom TCP`**
- Origen: por ejemplo, el identificador del grupo de seguridad de la aplicación que creó anteriormente en este tema: sg-9edd5cfb.

c. Seleccione Agregar regla.

d. Establezca los siguientes valores para la regla de entrada nueva con objeto de permitir el acceso HTTP a su aplicación.

- Tipo — **`HTTP`**
- Fuente — **`0.0.0.0/0`**

5. Para crear el grupo de seguridad, elija Create security group (Crear grupo de seguridad).

Paso 4: Crear un grupo de subredes

Un grupo de subredes es una colección de subredes que se crean en una VPC y que después se asignan a los clústeres. Los grupos de subredes le permiten especificar una VPC en particular cuando crea los clústeres.

Para crear un grupo de subredes

1. Identifique las subredes privadas de la base de datos en la VPC.

   a. Abra la consola de Amazon VPC en https://console.aws.amazon.com /vpc.

   b. Seleccione VPC Dashboard (Panel de control de VPC) y, a continuación, seleccione Subnets (Subredes).

   c. Anote la subred IDs de las subredes que creó en el paso 1 denominada, por ejemplo: 1-us-west-2a y 2-us-west-2b. example-subnet-private example-subnet-private Necesitará la subred al crear el grupo de subredes. IDs

2. Inicie sesión en y abra la Consola de administración de AWS consola de Amazon DocumentDB en https://console.aws.amazon.com /docdb.

   Asegúrese de conectarse a la consola de Amazon DocumentDB, no a la consola de Amazon VPC.

3. En el panel de navegación, elija Subnet groups (grupos de subredes).

4. Seleccione Crear.

5. En la página Crear grupo de subredes, establezca estos valores en la sección Detalles del grupo de subredes:
   - Nombre: **`example-db-subnet-group`**
   - Descripción — **`Instance security group`**
6. En la sección Configuración, establezca los siguientes valores:
   - VPC: elija la VPC que creó anteriormente, por ejemplo: vpc-example.
   - Zonas de disponibilidad: seleccione las dos zonas de disponibilidad creadas en el Paso 1. Ejemplo: us-west-2a y us-west-2b.
   - Subredes: elija las subredes privadas que creó en el Paso 1.
7. Seleccione Crear.

El nuevo grupo de subredes aparece en la lista de grupos de subredes de la consola de DocumentDB. Puede elegir el grupo de subredes para ver los detalles en el panel de detalles. Estos detalles incluyen todas las subredes asociadas al grupo.

> **Note**
>
> Si creó esta VPC para asociarla a un clúster de DocumentDB, cree el clúster siguiendo las instrucciones que se indican en Creación de un clúster de Amazon DocumentDB.

Eliminación de una VPC

Puede eliminar una VPC y los demás recursos que se utilizan en ella si ya no son necesarios.

> **Note**
>
> Si agregó recursos en la VPC que creó en este tema, es posible que primero tenga que eliminar estos para poder eliminar la VPC. Por ejemplo, estos recursos pueden incluir EC2 instancias de Amazon o clústeres de DocumentDB. Para obtener más información, consulte Eliminación de la VPC en la Guía del usuario de Amazon VPC.

Para eliminar una VPC y los recursos relacionados

1. Elimine el grupo de subredes:

a. Inicie sesión en y abra la Consola de administración de AWS consola de Amazon DocumentDB en https://console.aws.amazon.com /docdb.

b. En el panel de navegación, elija Subnet groups (grupos de subredes).

c. Seleccione el grupo de subredes que desee eliminar, por ejemplo. example-db-subnet-group

d. Elija Delete (Eliminar) y, a continuación, elija Delete (Eliminar) en la ventana de confirmación.

2. Anote el ID de la VPC:

a. Abra la consola de Amazon VPC en https://console.aws.amazon.com /vpc.

b. Elija el panel de control de VPC y, a continuación, elija el suyo. VPCs

c. En la lista, identifique la VPC que creó, como, por ejemplo, vpc-example.

d. Anote el ID de la VPC que ha creado. Necesitará el ID de la VPC en pasos posteriores.

3. Elimine los grupos de seguridad:

a. Abra la consola de Amazon VPC en https://console.aws.amazon.com /vpc.

b. Seleccione VPC Dashboard (Panel de control de VPC) y, a continuación, seleccione Security Groups (Grupos de seguridad).

c. Seleccione el grupo de seguridad del clúster de Amazon DocumentDB, como, por ejemplo, example-securitygroup.

d. En Acciones, elija Eliminar grupos de seguridad y, a continuación, seleccione Eliminar en el diálogo de confirmación.

e. De vuelta a la página Grupos de seguridad, selecciona el grupo de seguridad para la EC2 instancia de Amazon, como example-securitygroup.

f. En Acciones, elija Eliminar grupos de seguridad y, a continuación, seleccione Eliminar en el diálogo de confirmación.

4. Elimine la VPC:

a. Abra la consola de Amazon VPC en https://console.aws.amazon.com /vpc.

b. Elija el panel de control de VPC y, a continuación, elija el suyo. VPCs

c. Seleccione la VPC que desea eliminar, como, por ejemplo vpc-example.

d. En Acciones, elija Eliminar VPC.

La página de confirmación muestra otros recursos asociados a la VPC que también se eliminarán, incluidas las subredes asociadas a ella.

e. En el diálogo de confirmación, introduzca **`delete`** y, a continuación, elija Eliminar.

Creación de una VPC de pila doble para utilizarla con un clúster de DocumentDB

Una situación común incluye un clúster en una nube privada virtual (VPC) basada en el servicio Amazon VPC. Esta VPC comparte datos con una EC2 instancia pública de Amazon que se ejecuta en la misma VPC. En este tema, creará la VPC para esta situación.

Temas

- Paso 1: crear una VPC con subredes públicas y privadas
- Paso 2: Crear un grupo de seguridad de VPC para una instancia pública de Amazon EC2
- Paso 3: crear un grupo de seguridad de VPC para un clúster privado
- Paso 4: Crear un grupo de subredes
- Paso 5: Crear una EC2 instancia de Amazon en modo de doble pila
- Paso 6: crear un clúster en modo de pila doble
- Paso 7: Conéctese a la EC2 instancia de Amazon y al clúster de base de datos
- Elimine la VPC

En este procedimiento, creará la VPC para esta situación que funciona con una base de datos que se ejecuta en modo de pila doble. El modo de doble pila permite la conexión a través del IPv6 protocolo de direccionamiento. Para obtener más información sobre el direccionamiento de IP, consulte Direcciones IP de Amazon DocumentDB.

Los clústeres de red de pila doble se admiten en la mayoría de las regiones. Para obtener más información, consulte Disponibilidad del modo de pila doble según la región y versión. Para ver las limitaciones del modo de doble pila, consulte Limitaciones de los clústeres de red de pila doble.

Este tema y el tema IPv4 exclusivo crean las subredes públicas y privadas en la misma VPC. Para obtener información sobre cómo crear el clúster de Amazon DocumentDB en una VPC y la EC2 instancia de Amazon en una VPC diferente, consulte. Acceso a un clúster de Amazon DocumentDB en una VPC

Su clúster de DocumentDB debe estar disponible solo para su EC2 instancia de Amazon y no para la Internet pública. Además, cree de una VPC con subredes públicas y privadas. La EC2 instancia está alojada en la subred pública para que pueda acceder a la Internet pública. El clúster se aloja en una subred privada. La EC2 instancia se puede conectar al clúster porque está alojada en la misma VPC. Sin embargo, el clúster no está disponible en la Internet pública, lo que proporciona mayor seguridad.

Con los procedimientos de este tema, se configura una subred pública y privada adicional en una zona de disponibilidad independiente. El procedimiento no utiliza estas subredes. Los grupos de subredes de DocumentDB requieren una subred en, al menos, dos zonas de disponibilidad. La subred adicional facilita la configuración de más de una instancia de DocumentDB.

Para crear un clúster que utilice el modo de pila doble, especifique Modo de pila doble en el ajuste Tipo de red. También puede modificar un clúster con el mismo ajuste. Para obtener más información acerca de la creación de un clúster, consulte Creación de un clúster de Amazon DocumentDB. Para obtener más información sobre la modificación de un clúster de base de datos, consulte Modificación de un clúster de Amazon DocumentDB.

En este tema se describe la configuración de una VPC para clústeres de Amazon DocumentDB. Para obtener más información sobre Amazon VPC, consulte la Guía del usuario de Amazon VPC.

Paso 1: crear una VPC con subredes públicas y privadas

Utilice el siguiente procedimiento para crear una VPC con subredes públicas y privadas.

Para crear una VPC y subredes

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com /vpc.
2. En la esquina superior derecha de Consola de administración de AWS, elige la región en la que quieres crear tu VPC. En este ejemplo se utiliza la región Oeste de EE. UU. (Oregón).
3. En la esquina superior izquierda, elija VPC Dashboard (Panel de control VPC). Para comenzar a crear una VPC, elija Create VPC (Crear una VPC).
4. En Resources to create (Recursos para crear), en VPC settings (Configuración VPC), elija VPC and more (VPC y más).
5. En VPC settings (Configuración de la VPC), establezca estos valores:

   - Generación automática de etiquetas de identificación — **`example-dual-stack`**
   - IPv4 Bloque CIDR — **`10.0.0.0/16`**
   - IPv6 Bloque CIDR: bloque CIDR proporcionado por Amazon IPv6

- Tenencia: predeterminada
- Número de zonas de disponibilidad (): 2 AZs
- Personalizar AZs: mantenga los valores predeterminados
- Número de subredes públicas: 2
- Número de subredes privadas: 2
- Personalizar bloques de CIDR de subredes: conserve los valores predeterminados.
- Puertas de enlace NAT ($): ninguna
- Puerta de enlace de Internet solo de salida: no
- Puntos de conexión de VPC: ninguno
- Opciones de DNS: conserve los valores predeterminados.

6. Seleccione Creación de VPC.

Paso 2: Crear un grupo de seguridad de VPC para una instancia pública de Amazon EC2

Primero debe crear un grupo de seguridad para el acceso público. Para conectarse a las EC2 instancias públicas de la VPC, añada reglas de entrada al grupo de seguridad de la VPC que permitan que el tráfico se conecte desde Internet.

Para crear un grupo de seguridad de VPC

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com /vpc.
2. Elija VPC Dashboard (Panel VPC), seguido de Security Groups (Grupos de seguridad) y, por último, Create Security Group (Crear grupo de seguridad).
3. En la página Create Security Group (Crear grupo de seguridad), establezca estos valores:
   - Nombre del grupo de seguridad: **`example-dual-stack-securitygroup`**
   - Descripción — **`Dual-stack security group`**
   - VPC: elija la VPC que creó anteriormente, por ejemplo:. vpc-example-dual-stack
4. Agregar reglas de entrada al grupo de seguridad
   a. Determine la dirección IP que se utilizará para conectarse a EC2 las instancias de la VPC mediante Secure Shell (SSH). Para determinar su dirección IP pública, en otra ventana o pestaña del navegador, puede utilizar el servicio en. https://checkip.amazonaws.com

Un ejemplo de intervalo de direcciones del Protocolo de Internet versión 4 (IPv4) es`203.0.113.25/32`. Un ejemplo de intervalo de direcciones del Protocolo de Internet versión 6 (IPv6) es`2001:db8:1234:1a00::/64`.

En muchos casos, puede conectarse a través de un proveedor de internet (ISP) o protegido por un firewall sin una dirección IP estática. Si es así, busque el rango de direcciones IP utilizadas por los ordenadores cliente.

> **Warning**
>
> Si lo utilizas `0.0.0.0/0` para IPv4 o `::0` para IPv6, permites que todas las direcciones IP accedan a tus instancias públicas mediante SSH. Este método es aceptable para un periodo de tiempo corto en un entorno de prueba, pero no es seguro en entornos de producción. En los entornos de producción, debe autorizar el acceso a sus instancias únicamente a una dirección IP o a un rango de direcciones IP específicos.

b. En la sección Inbound rules (Reglas de entrada), elija Add rule (agregar regla).

c. Establece los siguientes valores para tu nueva regla de entrada para permitir el acceso de SSH a tu instancia de Amazon EC2 . Una vez hecho esto, puedes conectarte a tu EC2 instancia para instalar aplicaciones u otras utilidades. Especifica una dirección IP para poder acceder a la EC2 instancia:

- Escriba — **`SSH`**
- Origen: la dirección IP o el rango que creó en el Paso a. Un ejemplo de rango de IPv4 direcciones es **`203.0.113.25/3`** 2. Un ejemplo de rango de IPv6 direcciones es**`2001:DB8::/32`**.

d. Seleccione Agregar regla.

5. Para crear el grupo de seguridad, elija Create security group (Crear grupo de seguridad).

   Anote el identificador del grupo de seguridad, ya que lo necesitará más tarde en otro procedimiento.

Paso 3: crear un grupo de seguridad de VPC para un clúster privado

Para crear un clúster privado, debe crear un segundo grupo de seguridad para el acceso privado. Para conectarse a clústeres privados en su VPC, añada reglas de entrada a su grupo de seguridad de VPC. Solo permiten el tráfico desde tu EC2 instancia de Amazon.

Para crear un grupo de seguridad de VPC

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com /vpc.
2. Elija VPC Dashboard (Panel VPC), seguido de Security Groups (Grupos de seguridad) y, por último, Create Security Group (Crear grupo de seguridad).
3. En la página Create Security Group (Crear grupo de seguridad), establezca estos valores:
   - Nombre del grupo de seguridad: **`example-dual-stack-cluster-securitygroup`**
   - Descripción — **`Dual-stack cluster security group`**
   - VPC: elija la VPC que creó anteriormente, por ejemplo: vpc-example-dual-stack
4. Agregar reglas de entrada al grupo de seguridad
   a. En la sección Inbound rules (Reglas de entrada), elija Add rule (gregar regla).
   b. Defina los siguientes valores para la nueva regla de entrada a fin de permitir el tráfico de DocumentDB en el puerto 27017 desde su instancia de Amazon. EC2 Una vez hecho esto, puede conectarse desde la EC2 instancia al clúster. De este modo, puedes enviar datos de tu EC2 instancia a tu base de datos.
      - Escriba — **`Custom TCP`**
      - Origen: el identificador del grupo de EC2 seguridad que creó anteriormente en este tema, por ejemplo: sg-9edd5cfb.
5. Para crear el grupo de seguridad, elija Create security group (Crear grupo de seguridad).

Paso 4: Crear un grupo de subredes

Un grupo de subredes es una colección de subredes que se crean en una VPC y que después se asignan a los clústeres. Un grupo de subredes le permite especificar una VPC específica cuando crea clústeres. Para crear un grupo de subredes que sea compatible con `DUAL`, todas las subredes deben ser compatibles con `DUAL`. Para ser `DUAL` compatible, una subred debe tener un IPv6 CIDR asociado.

Para crear un grupo de subredes

1. Identifique las subredes privadas de la base de datos en la VPC.

   a. Abra la consola de Amazon VPC en https://console.aws.amazon.com /vpc.

   b. Seleccione VPC Dashboard (Panel de control de VPC) y, a continuación, seleccione Subnets (Subredes).

   c. Anote la subred IDs de las subredes que creó en el paso 1 denominada, por ejemplo: -private1-us-west-2a y -private2-us-west-2b. example-dual-stack-subnet example-dual-stack-subnet Necesitará IDs la subred al crear el grupo de subredes.

2. Inicie sesión en y abra la Consola de administración de AWS consola de Amazon DocumentDB en https://console.aws.amazon.com /docdb.

   Asegúrese de conectarse a la consola de Amazon DocumentDB, no a la consola de Amazon VPC.

3. En el panel de navegación, elija Subnet groups (grupos de subredes).

4. Seleccione Crear.

5. En la página Crear grupo de subredes, establezca estos valores en la sección Detalles del grupo de subredes:

   - Nombre: **`example-dual-stack-cluster-subnet-group`**
   - Descripción — **`Dual-stack cluster subnet group`**

6. En la sección Configuración, establezca los siguientes valores:

   - VPC: elija la VPC que creó anteriormente, por ejemplo: vpc-example-dual-stack
   - Zonas de disponibilidad: seleccione las dos zonas de disponibilidad creadas en el Paso 1. Ejemplo: us-west-2a y us-west-2b.
   - Subredes: elija las subredes privadas que creó en el Paso 1.

7. Seleccione Crear.

El nuevo grupo de subredes aparece en la lista de grupos de subredes de la consola de DocumentDB. Puede elegir el grupo de subredes para ver los detalles en el panel de detalles. Estos detalles incluyen todas las subredes asociadas al grupo.

Paso 5: Crear una EC2 instancia de Amazon en modo de doble pila

Para crear una EC2 instancia de Amazon, sigue las instrucciones de Lanzar una EC2 instancia mediante el asistente de lanzamiento de instancias de la consola en la Guía del usuario de Amazon Elastic Compute Cloud.

En la página Configure Instance Details (Configurar detalles de instancia), defina estos valores y mantenga los demás con sus valores predeterminados:

- Red: elija una VPC existente con subredes públicas y privadas, como vpc-example-dual-stack-vpc (identificador de vpc) creada en. Paso 1: crear una VPC con subredes públicas y privadas
- Subred: elija una subred pública existente, como el identificador de subred | -public1-us-east-2a | us-east-2a creado en. example-dual-stack-subnet Paso 2: Crear un grupo de seguridad de VPC para una instancia pública de Amazon EC2
- Asignar automáticamente IP pública: elija Habilitar.
- IPv6 Asignación automática de IP: seleccione Activar.
- Firewall (grupos de seguridad): elija Seleccionar un grupo de seguridad existente.
- Grupos de seguridad comunes: elija un grupo de seguridad existente, como el example-dual-stack-securitygroupcreado enPaso 2: Crear un grupo de seguridad de VPC para una instancia pública de Amazon EC2 . Asegúrese de que el grupo de seguridad que elija incluya reglas de entrada para acceso Secure Shell (SSH) y HTTP.

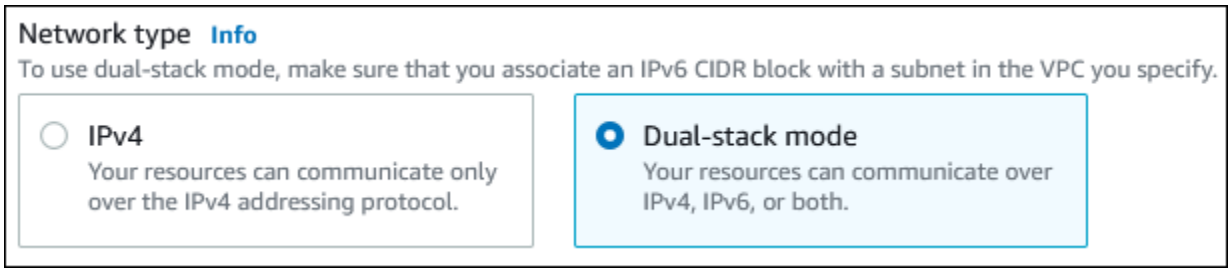
Paso 6: crear un clúster en modo de pila doble

En este paso, debe crear un clúster de base de datos que se ejecute en modo de pila doble. !!! Nota: ¡Esta sección necesita ser editada una vez que se hayan realizado las IPv6 actualizaciones en la consola!

Cómo crear un clúster en modo de pila doble

1. Inicie sesión en y abra la Consola de administración de AWS consola de Amazon DocumentDB en https://console.aws.amazon.com /docdb.
2. En la esquina superior derecha de la consola, elija el Región de AWS lugar en el que desee crear el clúster de DocumentDB. En este ejemplo se utiliza la región Este de EE. UU. (Ohio).
3. En el panel de navegación, seleccione Clusters (Clústeres).
4. En la página de lista de Clústeres, elija Crear.

5. En la página Crear clúster de Amazon DocumentDB, asegúrese de elegir la opción de clúster basado en instancias.
6. En la sección Conectividad, en Tipo de red, elija el modo de pila doble.



7. En la parte inferior de la página, active Mostrar configuración avanzada.
8. En la sección Configuración de la red, establezca los siguientes valores:

   - Nube privada virtual (VPC): elija una VPC existente con subredes públicas y privadas, como vpc-example-dual-stack(identificador de vpc) creada en. Paso 1: crear una VPC con subredes públicas y privadas

     La VPC debe tener subredes en diferentes zonas de disponibilidad.
   - Grupo de subredes: elija un grupo de subredes para la VPC, como example-dual-stack-cluster -subnet-group creado en. Paso 4: Crear un grupo de subredes
   - Acceso público: elija No.
   - Grupo de seguridad de VPC (firewall): seleccione Elegir existente.
   - Grupos de seguridad de VPC existentes: elija un grupo de seguridad de VPC existente que esté configurado para el acceso privado, como example-dual-stack-cluster -securitygroup creado en. Paso 3: crear un grupo de seguridad de VPC para un clúster privado

     Elimine otros grupos de seguridad, como el grupo de seguridad predeterminado, seleccionando la X asociada con cada uno de ellos.
   - Zonas de disponibilidad: seleccione la zona de disponibilidad creada en el Paso 1. Ejemplo: us-west-2a.

     Para evitar el tráfico entre zonas de disponibilidad, asegúrate de que el clúster y la EC2 instancia estén en la misma zona de disponibilidad.
9. En el resto de las secciones, especifique la configuración de su clúster. Para obtener más información acerca de cada configuración, consulte Creación de un clúster de Amazon DocumentDB.

Paso 7: Conéctese a la EC2 instancia de Amazon y al clúster de base de datos

Tras crear la EC2 instancia de Amazon y el clúster de DocumentDB en modo de doble pila, puede conectarse a cada uno de ellos mediante el protocolo. IPv6 Para conectarse a una EC2 instancia mediante el IPv6 protocolo, siga las instrucciones de Connect your EC2 instance en la Guía del usuario de Amazon Elastic Compute Cloud.

Para conectarse al clúster de DocumentDB desde la EC2 instancia, siga las instrucciones del tema Connect Amazon EC2 manualmente (y continúe con los pasos 6 y 7 siguientes del mismo procedimiento). Paso 5: instalación del intérprete de comandos de MongoDB

Elimine la VPC

Puede eliminar una VPC y los demás recursos que se utilizan en ella si ya no son necesarios.

> **Note**
>
> Si agregó recursos en la VPC que creó en este tema, es posible que primero tenga que eliminar estos para poder eliminar la VPC. Por ejemplo, estos recursos pueden incluir EC2 instancias de Amazon o clústeres de DocumentDB. Para obtener más información, consulte Eliminación de la VPC en la Guía del usuario de Amazon VPC.

Para eliminar una VPC y los recursos relacionados

1. Elimine el grupo de subredes:
   a. Inicie sesión en y abra la Consola de administración de AWS consola de Amazon DocumentDB en https://console.aws.amazon.com /docdb.
   b. En el panel de navegación, elija Subnet groups (grupos de subredes).
   c. Seleccione el grupo de subredes que desee eliminar, como -subnet-group. example-dual-stack-cluster
   d. Elija Delete (Eliminar) y, a continuación, elija Delete (Eliminar) en la ventana de confirmación.
2. Anote el ID de la VPC:
   a. Abra la consola de Amazon VPC en https://console.aws.amazon.com /vpc.
   b. Elija el panel de control de VPC y, a continuación, elija el suyo. VPCs

c. En la lista, identifique la VPC que creó, por ejemplo. vpc-example-dual-stack

d. Anote el ID de la VPC que ha creado. Necesitará el ID de la VPC en pasos posteriores.

3. Elimine los grupos de seguridad:

a. Abra la consola de Amazon VPC en https://console.aws.amazon.com /vpc.

b. Seleccione VPC Dashboard (Panel de control de VPC) y, a continuación, seleccione Security Groups (Grupos de seguridad).

c. Seleccione el grupo de seguridad para el clúster de Amazon DocumentDB, por ejemplo. example-dual-stack-securitygroup

d. En Acciones, elija Eliminar grupos de seguridad y, a continuación, seleccione Eliminar en el diálogo de confirmación.

e. De vuelta a la página Grupos de seguridad, selecciona el grupo de seguridad para la EC2 instancia de Amazon, como example-securitygroup.

f. En Acciones, elija Eliminar grupos de seguridad y, a continuación, seleccione Eliminar en el diálogo de confirmación.

4. Elimine la puerta de enlace NAT:

a. Abra la consola de Amazon VPC en https://console.aws.amazon.com /vpc.

b. Seleccione VPC Dashboard (Panel de control de VPC) y, a continuación, seleccione Security Groups (Grupos de seguridad).

c. Seleccione la puerta de enlace NAT de la VPC que creó. Utilice el ID de VPC para identificar la puerta de enlace NAT correcta.

d. En Actions (Acciones), seleccione Delete NAT gateway (Eliminar puerta de enlace NAT).

e. En el diálogo de confirmación, introduzca **`delete`** y, a continuación, elija Eliminar.

5. Elimine la VPC:

a. Abra la consola de Amazon VPC en https://console.aws.amazon.com /vpc.

b. Elija el panel de control de VPC y, a continuación, elija el suyo. VPCs

c. Seleccione la VPC que desee eliminar, por ejemplo. vpc-example-dual-stack

d. En Acciones, elija Eliminar VPC.

La página de confirmación muestra otros recursos asociados a la VPC que también se eliminarán, incluidas las subredes asociadas a ella.

e. En el diálogo de confirmación, introduzca **`delete`** y, a continuación, elija Eliminar.

6. Lance la dirección IP elástica.

   a. Abra la EC2 consola en https://console.aws.amazon.com/ec2.

   b. Elige EC2 Dashboard y, a continuación, Elastic. IPs

   c. Seleccione la dirección IP elástica que desea liberar.

   d. Desde Actions (Acciones), elija Release Elastic IP addresses (Liberar direcciones IP elásticas).

   e. En el cuadro de diálogo de confirmación, elija Lanzar.

Copia de seguridad y restauración en Amazon DocumentDB

Amazon DocumentDB (compatible con MongoDB) crea copias de seguridad de datos de forma continua en Amazon Simple Storage Service (Amazon S3) durante un periodo de 1 a 35 días para que se pueda restaurar con rapidez a cualquier punto dentro del periodo de retención de copia de seguridad. Amazon DocumentDB también toma instantáneas automáticas de los datos como parte de este proceso de copia de seguridad continua.

> **Note**
>
> Se trata de buckets de Amazon S3 administrados por servicios, por lo que usted no tendrá acceso a los archivos de copia de seguridad. Si desea controlar sus propias copias de seguridad, siga las instrucciones de volcado, restauración, importación y exportación de datos.

También puede conservar los datos de las copias de seguridad después del periodo de retención de copia de seguridad creando una instantánea manual de los datos del clúster. El proceso de copia de seguridad no afecta al rendimiento del clúster.

En esta sección se explican los casos de uso de las funciones de copia de seguridad de Amazon DocumentDB y se muestra cómo administrar las copias de seguridad de los clústeres de Amazon DocumentDB.

Temas

- Conceptos de copia de seguridad y restauración
- Descripción del uso de almacenamiento de copias de seguridad en
- Volcado, restauración, importación y exportación de datos
- Consideraciones sobre las instantáneas de clústeres
- Diferencias entre las instantáneas automáticas y manuales
- Creación de una instantánea manual del clúster
- Copia de instantáneas de clústeres de Amazon DocumentDB
- Uso compartido de instantáneas de clústeres de Amazon DocumentDB
- Restauración de una instantánea del clúster

- Restauración a un momento dado
- Eliminación de una instantánea del clúster

Conceptos de copia de seguridad y restauración

Nombre	Description (Descripción)	APIs (Verbos)

Backup retention period (Periodo de retención de copia de seguridad)	Periodo de tiempo comprendido entre 1 y 35 días durante el que se puede realizar una point-in-time restauración.	`create-db-cluster`
		`modify-db-cluster`
		`restore-db-cluster-to-point-in-time`

Volumen de almacenamiento de Amazon DocumentDB	Volumen de almacenamiento de alta disponibilidad y larga duración que replica los datos de seis formas	`create-db-cluster` `delete-db-cluster`

Nombre	Description (Descripción)	APIs (Verbos)
	en tres zonas de disponibilidad. Los clústeres de Amazon DocumentDB son de larga duración independientemente del número de instancias en el clúster.	

Intervalo de copia de seguridad	Periodo de tiempo en el día en el que se realizan las instantáneas automáticas.	`create-db-cluster`
		`describe-db-cluster`
		`modify-db-cluster`

Nombre	Description (Descripción)	APIs (Verbos)

Instantánea automática	Instantáneas diarias que son copias de seguridad completas del clúster y que se crean automáticamente mediante el proceso de copia de seguridad continua de Amazon DocumentDB.	`restore-db-cluster-from-snapshot`
		
		`describe-db-cluster-snapshot-attributes`
		
		`describe-db-cluster-snapshots`

Nombre	Description (Descripción)	APIs (Verbos)

Instantánea manual	Instantáneas que crea manualmente para conservar copias de seguridad completas de un clúster más allá del periodo de copia de seguridad.	`create-db-cluster-snapshot`
		`copy-db-cluster-snapshot`
		`delete-db-cluster-snapshot`
		`describe-db-cluster-snapshot-attributes`
		`describe-db-cluster-snapshots`
		`modify-db-cluster-snapshot-attribute`

Descripción del uso de almacenamiento de copias de seguridad en

El almacenamiento de copias de seguridad de Amazon DocumentDB se compone de copias de seguridad continuas durante el periodo de retención de copia de seguridad y de instantáneas manuales fuera del periodo de retención. Para controlar el uso de almacenamiento de copias de seguridad, puede reducir el intervalo de retención de copia de seguridad, eliminar las instantáneas manuales anteriores cuando ya no las necesite o ambas cosas. Para obtener información general acerca de las copias de seguridad de Amazon DocumentDB, consulte Copia de seguridad y restauración en Amazon DocumentDB. Para obtener información acerca de los precios del almacenamiento de copias de seguridad de Amazon DocumentDB, consulte la página web Precios de Amazon DocumentDB.

Para controlar los costos, puede monitorizar la cantidad de almacenamiento consumido por las copias de seguridad continuas y las instantáneas manuales que persistan más allá del periodo de retención. A continuación, puede reducir el intervalo de retención de copia de seguridad y eliminar las instantáneas manuales cuando ya no las necesite.

Puede utilizar las CloudWatch métricas `TotalBackupStorageBilled` de Amazon y revisar y `BackupRetentionPeriodStorageUsed` supervisar la cantidad de almacenamiento que utilizan sus copias de seguridad de Amazon DocumentDB, de la siguiente manera: `SnapshotStorageUsed`

- `BackupRetentionPeriodStorageUsed` representa la cantidad de almacenamiento de copias de seguridad utilizado para almacenar copias de seguridad continuas en el momento actual. El valor de esta métrica depende del tamaño del volumen del clúster y de la cantidad de cambios que realice durante el periodo de retención. Sin embargo, a efectos de facturación, la métrica no supera el tamaño del volumen del clúster acumulado durante el periodo de retención. Por ejemplo, si el tamaño del clúster es de 100 GiB y el periodo de retención es de dos días, el valor máximo de `BackRetentionPeriodStorageUsed` es 200 GiB (100 GiB + 100 GiB).

- `SnapshotStorageUsed` representa la cantidad de almacenamiento de copias de seguridad utilizado para almacenar instantáneas manuales más allá del periodo de retención de copia de seguridad. Las instantáneas manuales realizadas en el periodo de retención no cuentan para el almacenamiento de copias de seguridad. Asimismo, las instantáneas automáticas tampoco cuentan para el almacenamiento de copias de seguridad. El tamaño de cada instantánea es el tamaño del volumen del clúster en el momento en que se realiza la instantánea. El valor de `SnapshotStorageUsed` depende del número de instantáneas que mantiene y del tamaño de cada instantánea. Suponga, por ejemplo, que tiene una instantánea fuera del periodo de retención y que el volumen del clúster tenía un tamaño de 100 GiB cuando se realizó la instantánea. La cantidad de `SnapshotStorageUsed` es 100 GiB.

- `TotalBackupStorageBilled` representa la suma de `BackupRetentionPeriodStorageUsed` y `SnapshotStorageUsed`, menos una cantidad de almacenamiento gratuita de copias de seguridad equivalente al tamaño del volumen de un clúster de un día. Por ejemplo, si el tamaño del clúster es de 100 GiB, tiene un día de retención y hay una instantánea fuera del periodo de retención, `TotalBackupStorageBilled` será 100 GiB (100 GiB + 100 GiB - 100 GiB).

- Estas métricas se calculan de forma independiente para cada clúster de Amazon DocumentDB.

Puede monitorizar sus clústeres de Amazon DocumentDB y crear informes mediante CloudWatch métricas a través de la CloudWatch consola. Para obtener más información sobre cómo usar CloudWatch las métricas, consulteMonitorización de Amazon DocumentDB.

Volcado, restauración, importación y exportación de datos

Puede utilizar las utilidades `mongodump`, `mongorestore`, `mongoexport` y `mongoimport` para mover datos dentro y fuera del clúster de Amazon DocumentDB. En esta sección se analiza la finalidad de cada una de estas herramientas y configuraciones para ayudarle a lograr un mejor rendimiento.

Temas

- mongodump
- mongorestore
- mongoexport
- mongoimport
- Tutorial

`mongodump`

La utilidad `mongodump` crea una copia de seguridad binaria (BSON) de una base de datos MongoDB. La herramienta `mongodump` es el método preferido para volcar datos de su implementación de MongoDB de origen cuando busca restaurarla en su clúster de Amazon DocumentDB debido a las eficiencias de tamaño logradas al almacenar los datos en un formato binario.

En función de los recursos disponibles en la instancia o el equipo que esté utilizando para ejecutar el comando, puede acelerar su `mongodump` aumentando el número de colecciones paralelas volcadas desde el valor predeterminado 1 utilizando la opción `--numParallelCollections`. Una buena sugerencia es comenzar con un proceso de trabajo por vCPU en la instancia principal del clúster de Amazon DocumentDB.

> **Note**
>
> Recomendamos las herramientas de base de datos de MongoDB hasta la versión 100.6.1 inclusive para Amazon DocumentDB. Puede acceder a las descargas de las herramientas de base de datos de MongoDB aquí.

Ejemplo de uso

A continuación se muestra un ejemplo de uso de la utilidad `mongodump` en el clúster de Amazon DocumentDB, `sample-cluster`.

```
mongodump --ssl \
    --host="sample-cluster.node.us-east-1.docdb.amazonaws.com:27017" \
    --collection=sample-collection \
    --db=sample-database \
    --out=sample-output-file \
    --numParallelCollections 4  \
    --username=sample-user \
    --password=abc0123 \
    --sslCAFile global-bundle.pem
```

`mongorestore`

La utilidad `mongorestore` permite restaurar una copia de seguridad binaria (BSON) de una base de datos creada con la utilidad `mongodump`. Puede mejorar el rendimiento de la restauración aumentando el número de procesos de trabajo para cada colección durante la restauración con la opción `--numInsertionWorkersPerCollection` (el valor predeterminado es 1). Una buena sugerencia es comenzar con un proceso de trabajo por vCPU en la instancia principal del clúster de Amazon DocumentDB.

Ejemplo de uso

A continuación se muestra un ejemplo de uso de la utilidad `mongorestore` en el clúster de Amazon DocumentDB, `sample-cluster`.

```
mongorestore --ssl \
    --host="sample-cluster.node.us-east-1.docdb.amazonaws.com:27017" \
    --username=sample-user \
    --password=abc0123 \
```

```
    --sslCAFile global-bundle.pem <fileToBeRestored>
```

mongoexport

La herramienta `mongoexport` exporta datos en Amazon DocumentDB a formatos de archivo JSON, CSV o TSV. La herramienta `mongoexport` es el método preferido para exportar datos que deben ser legibles para las personas o máquinas.

> **Note**
>
> `mongoexport` no admite directamente las exportaciones paralelas. Sin embargo, es posible aumentar el rendimiento ejecutando varios trabajos `mongoexport` simultáneamente para distintas colecciones.

Ejemplo de uso

A continuación se muestra un ejemplo de uso de la herramienta `mongoexport` en el clúster de Amazon DocumentDB, `sample-cluster`.

```
mongoexport --ssl \
    --host="sample-cluster.node.us-east-1.docdb.amazonaws.com:27017" \
    --collection=sample-collection \
    --db=sample-database \
    --out=sample-output-file \
    --username=sample-user \
    --password=abc0123 \
    --sslCAFile global-bundle.pem
```

mongoimport

La herramienta `mongoimport` importa el contenido de los archivos JSON, CSV o TSV en un clúster de Amazon DocumentDB. Puede utilizar el parámetro `--numInsertionWorkers` para paralelizar y acelerar la importación (el valor predeterminado es 1).

Ejemplo de uso

A continuación se muestra un ejemplo de uso de la herramienta `mongoimport` en el clúster de Amazon DocumentDB, `sample-cluster`.

```
mongoimport --ssl \
    --host="sample-cluster.node.us-east-1.docdb.amazonaws.com:27017" \
    --collection=sample-collection \
    --db=sample-database \
    --file=<yourFile> \
    --numInsertionWorkers 4 \
    --username=sample-user \
    --password=abc0123 \
    --sslCAFile global-bundle.pem
```

Tutorial

En el siguiente tutorial se describe cómo utilizar las utilidades `mongodump`, `mongorestore`, `mongoexport` y `mongoimport` para mover datos dentro y fuera de un clúster de Amazon DocumentDB.

1. Requisitos previos: antes de empezar, asegúrese de que su clúster de Amazon DocumentDB está aprovisionado y de que tiene acceso a una instancia de EC2 Amazon en la misma VPC que su clúster. Para obtener más información, consulte Connect mediante Amazon EC2.

   Para poder utilizar las herramientas de utilidad mongo, debe tener el mongodb-org-tools paquete instalado en la instancia, de la siguiente manera. EC2

   ```
   sudo yum install mongodb-org-tools-4.0.18
   ```

   Dado que Amazon DocumentDB utiliza el cifrado de seguridad de la capa de transporte (TLS) de forma predeterminada, también debe descargar el archivo de la autoridad de certificación (CA) de Amazon RDS para utilizar el intérprete de comandos de mongo para conectarse, como se indica a continuación.

   ```
   wget https://truststore.pki.rds.amazonaws.com/global/global-bundle.pem
   ```

2. Descarga de datos de muestra: para este tutorial, descargará algunos datos de muestra que contienen información sobre restaurantes.

   ```
   wget https://raw.githubusercontent.com/ozlerhakan/mongodb-json-files/master/
   datasets/restaurant.json
   ```

3. Importación de los datos de muestra a Amazon DocumentDB: dado que los datos están en un formato JSON lógico, utilizará la utilidad `mongoimport` para importar los datos a su clúster de Amazon DocumentDB.

```
mongoimport --ssl \
    --host="tutorialCluster.amazonaws.com:27017" \
    --collection=restaurants \
    --db=business \
    --file=restaurant.json \
    --numInsertionWorkers 4 \
    --username=<yourUsername> \
    --password=<yourPassword> \
    --sslCAFile global-bundle.pem
```

4. Volcado de los datos con **`mongodump`**: ahora que tiene datos en su clúster de Amazon DocumentDB, puede realizar un volcado binario de esos datos mediante la utilidad `mongodump`.

```
mongodump --ssl \
    --host="tutorialCluster.us-east-1.docdb.amazonaws.com:27017"\
    --collection=restaurants \
    --db=business \
    --out=restaurantDump.bson \
    --numParallelCollections 4 \
    --username=<yourUsername> \
    --password=<yourPassword> \
    --sslCAFile global-bundle.pem
```

5. Eliminación de la colección **`restaurants`**: antes de restaurar la colección `restaurants` en la base de datos `business`, primero debe eliminar la colección que ya existe en esa base de datos, de la siguiente manera.

```
use business
```

```
db.restaurants.drop()
```

6. Restauración de los datos con **`mongorestore`**: con el volcado binario de los datos del paso 3, ahora puede usar la utilidad `mongorestore` para restaurar los datos en su clúster de Amazon DocumentDB.

```
mongorestore --ssl \
    --host="tutorialCluster.us-east-1.docdb.amazonaws.com:27017" \
```

```
    --numParallelCollections 4 \
    --username=<yourUsername> \
    --password=<yourPassword> \
    --sslCAFile global-bundle.pem restaurantDump.bson
```

7. Exportación de los datos mediante **`mongoexport`**: para completar el tutorial, exporte los datos del clúster en el formato de un archivo JSON, igual que con el archivo que importó en el paso 1.

```
mongoexport --ssl \
    --host="tutorialCluster.node.us-east-1.docdb.amazonaws.com:27017" \
    --collection=restaurants \
    --db=business \
    --out=restaurant2.json \
    --username=<yourUsername> \
    --password=<yourPassword> \
    --sslCAFile global-bundle.pem
```

8. Validación: puede validar que el resultado del paso 5 genera el mismo resultado que el del paso 1 con los siguientes comandos.

```
wc -l restaurant.json
```

Salida de este comando:

```
2548 restaurant.json
```

```
wc -l restaurant2.json
```

Salida de este comando:

```
2548 restaurant2.json
```

Consideraciones sobre las instantáneas de clústeres

Amazon DocumentDB crea instantáneas automáticas diarias del clúster durante el período de copia de seguridad del clúster. Amazon DocumentDB guarda las instantáneas automáticas del clúster en función del periodo de retención de copia de seguridad que haya especificado. Si es necesario, puede restaurar el clúster a cualquier momento dado durante el período de retención de copia de

seguridad. Las instantáneas automáticas no se producen mientras una copia se está ejecutando en la misma región del mismo clúster.

Temas

- Almacenamiento de copia de seguridad
- Intervalo de copia de seguridad
- Backup retention period (Periodo de retención de copia de seguridad)
- Copia del cifrado de instantáneas de clúster

Además de instantáneas automáticas del clúster, también puede crear manualmente una instantánea del clúster. Puede copiar tanto las instantáneas automáticas como las manuales. Para obtener más información, consulte Creación de una instantánea manual del clúster y Copia de instantáneas de clústeres de Amazon DocumentDB.

> **Note**
>
> El clúster debe estar en estado disponible para que se pueda realizar una instantánea automática.
> No se pueden compartir instantáneas automatizadas de un clúster de Amazon DocumentDB. Como solución alternativa, puede crear una instantánea manual copiando la instantánea automatizada y compartir después esa copia. Para obtener más información acerca de cómo copiar una instantánea, consulte Copia de instantáneas de clústeres de Amazon DocumentDB. Para obtener más información acerca de cómo restaurar un clúster desde una instantánea, consulte Restauración de una instantánea del clúster.

Almacenamiento de copia de seguridad

El almacenamiento de copias de seguridad de Amazon DocumentDB para cada una de ellas Región de AWS está compuesto por el almacenamiento de copias de seguridad necesario para el período de retención de copias de seguridad, que incluye instantáneas de clústeres automáticas y manuales en esa región. El período predeterminado de retención de copia de seguridad es de un día. Para obtener más información acerca de los precios del almacenamiento de copias de seguridad, consulte Precios de Amazon DocumentDB.

Al eliminar un clúster, se eliminan todas las instantáneas automáticas y no se pueden recuperar. Sin embargo, las instantáneas manuales no se eliminan al eliminar un clúster. Si decide hacer que

Amazon DocumentDB cree una instantánea final (instantánea manual) antes de eliminar el clúster, puede utilizar la instantánea final para recuperar el clúster.

Para obtener más información acerca de las instantáneas y el almacenamiento, consulte Descripción del uso de almacenamiento de copias de seguridad en .

Intervalo de copia de seguridad

Las instantáneas automáticas se realizan a diario durante el periodo de copia de seguridad preferido. Si la instantánea requiere más tiempo del asignado al periodo de copia de seguridad, el proceso de copia de seguridad continúa hasta que finaliza, aunque haya terminado el periodo de copia de seguridad. El periodo de copia de seguridad no se puede solapar con el periodo de mantenimiento semanal del clúster.

Si no especifica un periodo de copia de seguridad preferido al crear el clúster, Amazon DocumentDB asigna un período de copia de seguridad predeterminado de 30 minutos. Este periodo se elige al azar de un bloque de tiempo de 8 horas asociado a la región de su clúster. Puede cambiar el periodo de copia de seguridad preferido modificando el clúster. Para obtener más información, consulte Modificación de un clúster de Amazon DocumentDB.

Nombre de la región	Region	Bloque de tiempo en UTC
Este de EE. UU. (Ohio)	us-east-2	03:00-11:00
Este de EE. UU. (Norte de Virginia)	us-east-1	03:00-11:00
Oeste de EE. UU. (Oregón)	us-west-2	06:00-14:00
África (Ciudad del Cabo)	af-south-1	03:00-11:00
Asia-Pacífico (Hong Kong)	ap-east-1	06:00-14:00
Asia-Pacífico (Hyderabad)	ap-south-2	06:30–14:30
Asia-Pacífico (Malasia)	ap-southeast-5	13:00-21:00
Asia-Pacífico (Mumbai)	ap-south-1	06:00-14:00
Asia-Pacífico (Osaka)	ap-northeast-3	12:00–20:00

Nombre de la región	Region	Bloque de tiempo en UTC
Asia-Pacífico (Seúl)	ap-northeast-2	13:00-21:00
Asia-Pacífico (Singapur)	ap-southeast-1	14:00–22:00
Asia-Pacífico (Sídney)	ap-southeast-2	12:00–20:00
Asia-Pacífico (Yakarta)	ap-southeast-3	08:00-16:00
Asia-Pacífico (Tailandia)	ap-southeast-7	15:00-23:00
Asia-Pacífico (Tokio)	ap-northeast-1	13:00-21:00
Canadá (centro)	ca-central-1	03:00-11:00
China (Pekín)	cn-north-1	06:00-14:00
China (Ningxia)	cn-northwest-1	06:00-14:00
Europa (Fráncfort)	eu-central-1	21:00-05:00
Europa (Irlanda)	eu-west-1	22:00-06:00
Europa (Londres)	eu-west-2	22:00-06:00
Europa (Milán)	eu-south-1	02:00-10:00
Europa (París)	eu-west-3	23:59-07:29
Europa (España)	eu-south-2	02:00-10:00
Europa (Estocolmo)	eu-north-1	04:00 — 12:00
México (centro)	mx-central-1	03:00-11:00
Medio Oriente (EAU)	me-central-1	05:00-13:00
América del Sur (São Paulo)	sa-east-1	00:00-08:00
Israel (Tel Aviv)	il-central-1	04:00-12:00

Nombre de la región	Region	Bloque de tiempo en UTC
AWS GovCloud (Este de EE. UU.)	us-gov-east-1	17:00-01:00
AWS GovCloud (Estados Unidos-Oeste)	us-gov-west-1	06:00-14:00

Backup retention period (Periodo de retención de copia de seguridad)

El periodo de retención de copia de seguridad es el número de días que se conserva una copia de seguridad automática antes de que se elimine automáticamente. Amazon DocumentDB admite un periodo de retención de copia de seguridad de 1 a 35 días.

Puede configurar el periodo de retención de copia de seguridad al crear el clúster. Si no configura explícitamente el periodo de retención de copia de seguridad, se asigna al clúster el valor predeterminado de un día. Tras crear un clúster, puede modificar el período de retención de la copia de seguridad modificando el clúster mediante el Consola de administración de AWS o el AWS CLI. Para obtener más información, consulte Modificación de un clúster de Amazon DocumentDB.

Copia del cifrado de instantáneas de clúster

El cifrado de clústeres e instantáneas se basa en una clave de cifrado de KMS. El ID de la clave de KMS es el Nombre de recurso de Amazon (ARN), el identificador de la clave de KMS o el alias de la clave de KMS de la clave de cifrado de KMS.

Se aplican las siguientes directrices y limitaciones:

- El cifrado se deduce del clúster al crear una instantánea. Si el clúster está cifrado, la instantánea de ese clúster se cifra con la misma clave de KMS. Si el clúster no está cifrado, la instantánea no estará cifrada.
- Si copia una instantánea del clúster cifrada desde la cuenta de Amazon Web Services, puede especificar un valor para `KmsKeyId` para cifrar la copia con una nueva clave de cifrado de KMS. Si no especifica ningún valor para `KmsKeyId`, la copia de la instantánea del clúster se cifra con la misma clave de KMS que la instantánea del clúster de origen.
- Si copia una instantánea del clúster cifrada que se ha compartido desde otra cuenta de Amazon Web Services, debe especificar un valor para `KmsKeyId`.

- Para copiar una instantánea de clúster cifrada a otra región de Amazon Web Services, establezca `KmsKeyId` al ID de clave de KMS que desee utilizar para cifrar la copia de la instantánea de clúster en la región de destino. Las claves de cifrado de KMS son específicas de la región de Amazon Web Services en la que se han creado, y no puede usar claves de cifrado de una región de Amazon Web Services en otra región de Amazon Web Services.
- Si intenta copiar un snapshot de clúster de base de datos sin cifrar y especificar un valor para el parámetro `KmsKeyId`, se devuelve un error.

Diferencias entre las instantáneas automáticas y manuales

A continuación se detallan las principales características de las instantáneas automáticas y manuales de Amazon DocumentDB (compatible con MongoDB).

Las instantáneas automáticas de Amazon DocumentDB tienen las siguientes principales características:

- Nomenclatura de las instantáneas automáticas: los nombres de las instantáneas automáticas siguen el patrón `rds:<cluster-name>-yyyy-mm-dd-hh-mm`, donde `yyyy-mm-dd-hh-mm` representa la fecha y la hora en la que se creó la instantánea.
- Se crean automáticamente según una programación: al crear o modificar un clúster, puede definir el periodo de retención de copia de seguridad como un valor entero comprendido entre 1 y 35 días. De forma predeterminada, los clústeres nuevos tienen un periodo de retención de copia de seguridad de un día. El periodo de retención de copia de seguridad define el número de días que se conservan las instantáneas automáticas antes de que se eliminen automáticamente. No se pueden deshabilitar las copias de seguridad automáticas en los clústeres de Amazon DocumentDB.

  Además de definir el periodo de retención de copia de seguridad, también configura el periodo de copia de seguridad, que es la hora del día a la que se crean las instantáneas automáticas.
- Eliminación de instantáneas automáticas: las instantáneas automáticas se eliminan cuando elimina el clúster de la instantánea automática. No se puede eliminar manualmente una instantánea automática.
- Son incrementales: durante el periodo de retención de copia de seguridad, se registran las actualizaciones de la base de datos, por lo que se mantiene un registro incremental de los cambios.

- Restauración desde una instantánea automática: puede restaurar los datos desde una instantánea automática mediante la Consola de administración de AWS o la AWS CLI. Al restaurar a partir de una instantánea mediante el AWS CLI, debe añadir las instancias por separado una vez que el clúster esté disponible.
- Uso compartido: no se puede compartir una instantánea de clúster automatizada de Amazon DocumentDB. Como solución alternativa, puede crear una instantánea manual copiando la instantánea automatizada y compartir después esa copia. Para obtener más información acerca de cómo copiar una instantánea, consulte Copia de instantáneas de clústeres de Amazon DocumentDB. Para obtener más información acerca de cómo restaurar un clúster desde una instantánea, consulte Restauración de una instantánea del clúster.
- Puede restaurar desde cualquier punto durante el periodo de retención de copia de seguridad: como las actualizaciones de la base de datos se registran de manera incremental, puede restaurar el clúster a cualquier punto en el tiempo durante el periodo de retención de copia de seguridad.

  Al restaurar desde una instantánea automática o desde una point-in-time restauración mediante el AWS CLI, debe añadir las instancias por separado una vez que el clúster esté disponible.

Las instantáneas manuales de Amazon DocumentDB tienen las siguientes características principales:

- Creadas bajo demanda: las instantáneas manuales de Amazon DocumentDB se crean bajo demanda mediante la consola de administración de Amazon DocumentDB o. AWS CLI
- Eliminación de una instantánea manual: una instantánea manual solo se elimina cuando se elimina de forma explícita mediante la consola de Amazon DocumentDB o la AWS CLI. Las instantáneas manuales no se eliminan cuando se elimina el clúster.
- Copias de seguridad completas: cuando se realiza una instantánea manual, se crea y se almacena una copia de seguridad completa de los datos del clúster.
- Nomenclatura de instantáneas manuales: usted especifica el nombre de la instantánea manual. Amazon DocumentDB no añade una marca `datetime` al nombre, por lo que debe añadir esa información si desea que se incluya en el nombre.
- Restauración desde una instantánea manual: puede restaurar los datos desde una instantánea manual mediante la consola o la AWS CLI. Al restaurar a partir de una instantánea mediante el AWS CLI, debe añadir las instancias por separado una vez que el clúster esté disponible.
- Service Quotas: está limitado a un máximo de 100 instantáneas manuales por cada Región de AWS una.

- Uso compartido: puede compartir instantáneas de clúster manuales, que las Cuentas de AWS autorizadas pueden copiar. Puede compartir instantáneas manuales cifradas o no cifradas. Para obtener más información acerca de cómo copiar una instantánea, consulte Copia de instantáneas de clústeres de Amazon DocumentDB.
- La restauración tiene lugar cuando se realiza la instantánea manual: cuando se restauran los datos desde una instantánea manual, la restauración tiene lugar cuando se realiza la instantánea manual.

  Al restaurar a partir de una instantánea mediante el AWS CLI, debe añadir las instancias por separado una vez que el clúster esté disponible.

Creación de una instantánea manual del clúster

Puede crear una instantánea manual mediante la opción Consola de administración de AWS o AWS CLI. El tiempo que tarda en crearse una instantánea varía en función del tamaño de sus bases de datos. Cuando cree una instantánea, debe hacer lo siguiente:

1. Identificar el clúster del que va a realizar una copia de seguridad.
2. Asignar un nombre a la instantánea. Esto le permite restaurarla más adelante.

Using the Consola de administración de AWS

Para crear una instantánea manual mediante el Consola de administración de AWS, puede seguir cualquiera de los siguientes métodos.

1. Método 1:

   1. Inicie sesión en y abra la Consola de administración de AWS consola de Amazon DocumentDB en https://console.aws.amazon.com /docdb.
   2. En el panel de navegación, elija Snapshots (Instantáneas).

      > **Tip**
      >
      > Si no ve el panel de navegación del lado izquierdo de la pantalla, seleccione el icono de menú
      > (≡)
      > en la esquina superior izquierda de la página.

3. En la página Snapshots (Instantáneas), elija Create (Crear).
4. En la página Create cluster snapshot (Crear instantánea del clúster):
   a. Identificador de clúster: en la lista desplegable de clústeres, elija el clúster del que desea crear una instantánea.
   b. Identificador de la instantánea: introduzca un nombre para la instantánea.

      Restricciones relativas a la nomenclatura de instantáneas:

      - Debe tener [1-255] letras, números o guiones.
      - El primer carácter debe ser una letra.
      - No puede terminar con un guion ni contener dos guiones consecutivos.
      - Debe ser único para todos los clústeres de Amazon RDS, Amazon Neptune y Amazon DocumentDB por cuenta de AWS y por región.

   c. Seleccione Crear.

2. Método 2:

1. Inicie sesión en y abra la Consola de administración de AWS consola de Amazon DocumentDB en https://console.aws.amazon.com /docdb.
2. En el panel de navegación, seleccione Clusters (Clústeres).

   > **Tip**
   >
   > Si no ve el panel de navegación del lado izquierdo de la pantalla, seleccione el icono de menú
   > (≡)
   > en la esquina superior izquierda de la página.

3. En la página Clusters (clústeres), elija el botón situado a la izquierda del clúster cuya instantánea desee crear.
4. En el menú Actions (Acciones), elija Take snapshot (Realizar instantánea).
5. En la página Create cluster snapshot (Crear instantánea del clúster):
   a. Identificador de la instantánea: introduzca un nombre para la instantánea.

      Restricciones relativas a la nomenclatura de instantáneas:

      - Debe tener [1-63] letras, números o guiones.
      - El primer carácter debe ser una letra.

- No puede terminar con un guion ni contener dos guiones consecutivos.
- Debe ser único para todos los clústeres de Amazon RDS, Amazon Neptune y Amazon DocumentDB por cuenta de AWS y por región.

b. Seleccione Crear.

Using the AWS CLI

Para crear una instantánea de clúster mediante el AWS CLI, utilice la `create-db-cluster-snapshot` operación con los siguientes parámetros.

Parameters

- **`--db-cluster-identifier`**: obligatorio. El nombre del clúster del que va a realizar una instantánea. Este clúster debe existir y estar disponible.
- **`--db-cluster-snapshot-identifier`**: obligatorio. El nombre de la instantánea manual que va a crear.

En el ejemplo siguiente, se crea una instantánea llamada `sample-cluster-snapshot` del clúster `sample-cluster`.

Para Linux, macOS o Unix:

```
aws docdb create-db-cluster-snapshot \
    --db-cluster-identifier sample-cluster \
    --db-cluster-snapshot-identifier sample-cluster-snapshot
```

Para Windows:

```
aws docdb create-db-cluster-snapshot ^
    --db-cluster-identifier sample-cluster ^
    --db-cluster-snapshot-identifier sample-cluster-snapshot
```

La salida de esta operación será similar a lo que se indica a continuación.

```
{
    "DBClusterSnapshot": {
        "AvailabilityZones": [
            "us-east-1a",
            "us-east-1b",
```

```
            "us-east-1c"
        ],
        "DBClusterSnapshotIdentifier": "sample-cluster-snapshot",
        "DBClusterIdentifier": "sample-cluster",
        "SnapshotCreateTime": "2020-04-24T04:59:08.475Z",
        "Engine": "docdb",
        "Status": "creating",
        "Port": 0,
        "VpcId": "vpc-abc0123",
        "ClusterCreateTime": "2020-01-10T22:13:38.261Z",
        "MasterUsername": "master-user",
        "EngineVersion": "4.0.0",
        "SnapshotType": "manual",
        "PercentProgress": 0,
        "StorageEncrypted": true,
        "KmsKeyId": "arn:aws:kms:us-east-1:<accountID>:key/sample-key",
        "DBClusterSnapshotArn": "arn:aws:rds:us-east-1:<accountID>:cluster-
snapshot:sample-cluster-snapshot"
    }
}
```

Copia de instantáneas de clústeres de Amazon DocumentDB

En Amazon DocumentDB, puede copiar instantáneas dentro de la misma Región de AWS o en una diferente. Región de AWS También puede copiar las instantáneas compartidas a su cuenta en la misma cuenta Región de AWS o en una diferente. Región de AWS Para obtener más información sobre cómo compartir instantáneas, consulte Uso compartido de instantáneas de clústeres de Amazon DocumentDB.

> **Note**
>
> Amazon DocumentDB le factura en función de la cantidad de datos de copias de seguridad e instantáneas que conserve y el periodo de tiempo que los conserve. Para obtener más información sobre el almacenamiento asociado con las copias de seguridad y las instantáneas de Amazon DocumentDB, consulte Descripción del uso de almacenamiento de copias de seguridad en . Para obtener información acerca de los precios del almacenamiento de Amazon DocumentDB, consulte Precios de Amazon DocumentDB.

Temas

- Copia de instantáneas compartidas
- Copiar instantáneas de un lado a otro Regiones de AWS
- Limitaciones
- Tratamiento del cifrado
- Consideraciones relativas al grupo de parámetros
- Copia de una instantánea de clúster

Copia de instantáneas compartidas

Puedes copiar las instantáneas que otras AWS cuentas hayan compartido contigo. Si va a copiar una instantánea cifrada que se ha compartido desde otra AWS cuenta, debe tener acceso a la clave de AWS KMS cifrado que se utilizó para cifrar la instantánea. Para obtener más información, consulte Tratamiento del cifrado.

Copiar instantáneas de un lado a otro Regiones de AWS

Al copiar una instantánea en una Región de AWS que es diferente de la instantánea de origen Región de AWS, cada copia es una instantánea completa. Una copia de la instantánea completa contiene todos los datos y metadatos necesarios para restaurar el clúster de Amazon DocumentDB.

Limitaciones

A continuación se indican algunas limitaciones al copiar instantáneas:

- Si elimina una instantánea de origen antes de que la instantánea de destino esté disponible, la copia de la instantánea puede generar un error. Compruebe que la instantánea de destino tiene el estado `AVAILABLE` antes de eliminar una instantánea de origen.
- Puede tener hasta cinco solicitudes de copia de instantánea en curso en una única región de destino por cuenta.
- En función de lo que se Regiones de AWS trate y de la cantidad de datos que se vayan a copiar, una copia instantánea entre regiones puede tardar horas en completarse. En algunos casos, puede haber un gran número de solicitudes de copia de instantáneas entre regiones desde una Región de AWS de origen determinada. En estos casos, Amazon DocumentDB podría poner en cola las nuevas solicitudes de copia entre regiones procedentes de esa fuente hasta que Región de AWS se completen algunas copias en curso. No se muestra ninguna información de progreso

sobre las solicitudes de copia mientras están en la cola. La información de progreso se muestra cuando comienza la copia.

Tratamiento del cifrado

Puede copiar una instantánea que haya sido cifrada con una clave de cifrado de AWS KMS . Si copia una instantánea cifrada, la copia de la instantánea se debe cifrar también. Si copia una instantánea cifrada dentro de la misma Región de AWS, puede cifrar la copia con la misma clave de AWS KMS cifrado que la instantánea original o puede especificar una clave de cifrado diferente. AWS KMS Si copia una instantánea cifrada de una región a otra, no podrá utilizar la misma clave de AWS KMS cifrado para la copia que se utilizó para la instantánea de origen, ya que AWS KMS las claves son específicas de cada región. En su lugar, debe especificar una AWS KMS clave válida en el destino Región de AWS n.

La instantánea de origen permanece cifrada durante todo el proceso de copia. Para obtener más información, consulte Protección de datos en Amazon DocumentDB.

> **Note**
>
> Para instantáneas del clúster de Amazon DocumentDB, no es posible cifrar una instantánea del clúster sin cifrar al copiar la instantánea.

Consideraciones relativas al grupo de parámetros

Cuando se copia una instantánea entre regiones, la copia no incluye el grupo de parámetros empleado por el clúster de Amazon DocumentDB. Al restaurar una instantánea para crear un nuevo clúster, ese clúster obtiene el grupo de parámetros predeterminado para el lugar en el Región de AWS que se creó. Para aplicar en el nuevo clúster los mismos parámetros que en el original, debe hacer lo siguiente:

1. En el destino Región de AWS, cree un grupo de parámetros del clúster de Amazon DocumentDB con la misma configuración que el clúster original. Si ya existe uno en el nuevo Región de AWS, puede usarlo.
2. Tras restaurar la instantánea en el destino Región de AWS, modifique el nuevo clúster de Amazon DocumentDB y añada el grupo de parámetros nuevo o existente del paso anterior. Para obtener más información, consulte Modificación de un clúster de Amazon DocumentDB.

Copia de una instantánea de clúster

Puede copiar un clúster de Amazon DocumentDB mediante el Consola de administración de AWS o el AWS CLI, de la siguiente manera.

Using the Consola de administración de AWS

Para hacer una copia de una instantánea de un clúster mediante el Consola de administración de AWS, complete los siguientes pasos. Este procedimiento funciona para copiar instantáneas de clústeres cifradas o no cifradas, en la misma región Región de AWS o en varias regiones.

1. Inicie sesión en y abra la Consola de administración de AWS consola de Amazon DocumentDB en https://console.aws.amazon.com /docdb.
2. En el panel de navegación, elija Instantáneas y, a continuación, el botón situado a la izquierda de la instantánea que desea restaurar.

   > **Tip**
   >
   > Si no ve el panel de navegación del lado izquierdo de la pantalla, seleccione el icono de menú
   > (≡)
   > en la esquina superior izquierda de la página.

3. En el menú Actions, elija Copy.
4. En la página Hacer una copia de una instantánea de clúster, rellene la sección Configuración.

   a. Región de destino: opcional. Para copiar la instantánea del clúster a otra Región de AWS, selecciónela en la región Región de AWS de destino.

   b. Nuevo identificador de instantánea: escriba un nombre para la nueva instantánea.

      Restricciones relativas a la nomenclatura de instantáneas de destino:

      - No se puede coincidir con el nombre de una instantánea existente.
      - Debe tener [1-63] letras, números o guiones.
      - El primer carácter debe ser una letra.
      - No puede terminar con un guion ni contener dos guiones consecutivos.
      - Debe ser único para todos los clústeres de Amazon RDS, Neptune y Amazon DocumentDB por región. Cuenta de AWS

c. Copiar etiquetas: para copiar las etiquetas que tenga en su instantánea de origen a la copia de su instantánea, elija Copiar etiquetas.

5. Complete la sección E. ncryption-at-rest

a. Cifrado en reposo: si la instantánea no está cifrada, estas opciones no estarán disponibles, porque no puede crear una copia sin cifrar a partir de una instantánea cifrada. Si la instantánea está cifrada, puede cambiar la que AWS KMS key se utiliza durante el cifrado en reposo.

Para obtener más información acerca del cifrado de las copias de instantáneas, consulte Copia del cifrado de instantáneas de clúster.

Para obtener más información sobre el cifrado en reposo, consulte Cifrado de datos en reposo de Amazon DocumentDB.

b. AWS KMS Clave: en la lista desplegable, elija una de las siguientes opciones:

- (predeterminado) aws/rds: el número de cuenta y el identificador AWS KMS clave aparecen siguiendo esta opción.
- < some-key-name > — Si ha creado una clave, aparece en la lista y está disponible para que la elija.
- Introducir un ARN de clave: en el cuadro ARN, escriba el nombre de recurso de Amazon (ARN) de la clave de AWS KMS . El formato del ARN es el siguiente: `arn:aws:kms:<region>:<accountID>:key/<key-id>` .

6. Para crear una copia de la instantánea seleccionada, elija Copy snapshot (Copiar instantánea). También puede seleccionar Cancelar si no desea hacer una copia de la instantánea.

Using the AWS CLI

Para realizar una copia de una instantánea de clúster sin cifrar mediante la AWS CLI, utilice la operación `copy-db-cluster-snapshot` con los siguientes parámetros. Si va a copiar la instantánea a otra Región de AWS, ejecute el comando en el Región de AWS que se copiará la instantánea.

- **`--source-db-cluster-snapshot-identifier`**: obligatorio. El identificador de la instantánea del clúster de la que se va a hacer una copia. Debe existir la instantánea del clúster y tener el estado disponible. Si está copiando la instantánea en otra Región de AWS o si está

copiando una instantánea de clúster compartida, este identificador debe estar en el formato ARN de la instantánea de clúster de origen. Este parámetro no distingue entre mayúsculas y minúsculas.

- **`--target-db-cluster-snapshot-identifier`**: obligatorio. El identificador de la nueva instantánea del clúster que se va a crear a partir de la instantánea del clúster de origen. Este parámetro no distingue entre mayúsculas y minúsculas.

  Restricciones relativas a la nomenclatura de instantáneas de destino:

  - No se puede coincidir con el nombre de una instantánea existente.
  - Debe tener [1-63] letras, números o guiones.
  - El primer carácter debe ser una letra.
  - No puede terminar con un guion ni contener dos guiones consecutivos.
  - Debe ser único para todos los clústeres de Amazon RDS, Neptune y Amazon DocumentDB por región. Cuenta de AWS
- **`--source-region`**— Si va a copiar la instantánea a otra Región de AWS, especifique desde dónde Región de AWS se copiará la instantánea del clúster cifrada.

  Si desea copiar la instantánea en otra Región de AWS y no especifica `--source-region`, debe especificar en su lugar la opción `pre-signed-url`. El `pre-signed-url` valor debe ser una URL que contenga una solicitud firmada en la versión 4 de Signature para que se llame a la `CopyDBClusterSnapshot` acción en la fuente desde la Región de AWS que se copia la instantánea del clúster. Para obtener más información sobre esto`pre-signed-url`, consulte Copy DBCluster Snapshot.
- **`--kms-key-id`**: identificador de la clave de KMS que se va a utilizar para cifrar la copia de la instantánea del clúster.

  Si va a copiar una instantánea de clúster cifrada en otra Región de AWS, este parámetro es obligatorio. Debe especificar una clave KMS para el destino Región de AWS.

  Si va a copiar una instantánea de clúster cifrada en el mismo Región de AWS, el parámetro AWS KMS clave es opcional. La copia de la instantánea del clúster se cifra con la misma AWS KMS clave que la instantánea del clúster de origen. Si desea especificar una nueva clave de AWS KMS cifrado para cifrar la copia, puede hacerlo mediante este parámetro.
- **`--copy-tags`**— Opcional. Las etiquetas y los valores que se van a copiar.

Para cancelar una operación de copia una vez que está en curso, elimine la instantánea del clúster de destino identificado por `--target-db-cluster-snapshot-identifier` o `TargetDBClusterSnapshotIdentifier` mientras esa instantánea del clúster está en el estado copying.

Example

Ejemplo 1: copia de una instantánea sin cifrar a la misma región

En el siguiente AWS CLI ejemplo, se crea una copia de `sample-cluster-snapshot` named `sample-cluster-snapshot-copy` in Región de AWS igual que la instantánea de origen. Cuando se crea la copia, todas las etiquetas de la instantánea original se copian en la copia de la instantánea.

Para Linux, macOS o Unix:

```
aws docdb copy-db-cluster-snapshot \
    --source-db-cluster-snapshot-identifier sample-cluster-snapshot \
    --target-db-cluster-snapshot-identifier sample-cluster-snapshot-copy \
    --copy-tags
```

Para Windows:

```
aws docdb copy-db-cluster-snapshot ^
    --source-db-cluster-snapshot-identifier sample-cluster-snapshot ^
    --target-db-cluster-snapshot-identifier sample-cluster-snapshot-copy ^
    --copy-tags
```

La salida de esta operación será similar a lo que se indica a continuación.

```
{
    "DBClusterSnapshot": {
        "AvailabilityZones": [
            "us-east-1a",
            "us-east-1b",
            "us-east-1c"
        ],
        "DBClusterSnapshotIdentifier": "sample-cluster-snapshot-copy",
        "DBClusterIdentifier": "sample-cluster",
        "SnapshotCreateTime": "2020-03-27T08:40:24.805Z",
        "Engine": "docdb",
        "Status": "copying",
```

```
        "Port": 0,
        "VpcId": "vpc-abcd0123",
        "ClusterCreateTime": "2020-01-10T22:13:38.261Z",
        "MasterUsername": "master-user",
        "EngineVersion": "4.0.0",
        "SnapshotType": "manual",
        "PercentProgress": 0,
        "StorageEncrypted": true,
        "KmsKeyId": "arn:aws:kms:us-east-1:111122223333:key/sample-key-id",
        "DBClusterSnapshotArn": "arn:aws:rds:us-east-1:111122223333:cluster-
snapshot:sample-cluster-snapshot-copy",
        "SourceDBClusterSnapshotArn": "arn:aws:rds:us-east-1:111122223333:cluster-
snapshot:sample-cluster-snapshot"
    }
}
```

Example

Ejemplo 2: Copiar una instantánea sin cifrar de un lado a otro Regiones de AWS

En el AWS CLI ejemplo siguiente se crea una copia de`sample-cluster-snapshot`, que tiene el ARN`arn:aws:rds:us-east-1:123456789012:cluster-snapshot:sample-cluster-snapshot`. Esta copia recibe el nombre `sample-cluster-snapshot-copy` name y es Región de AWS en la que se ejecuta el comando.

Para Linux, macOS o Unix:

```
aws docdb copy-db-cluster-snapshot \
    --source-db-cluster-snapshot-identifier arn:aws:rds:us-
east-1:123456789012:cluster-snapshot:sample-cluster-snapshot \
    --target-db-cluster-snapshot-identifier sample-cluster-snapshot-copy
```

Para Windows:

```
aws docdb copy-db-cluster-snapshot ^
    --source-db-cluster-snapshot-identifier arn:aws:rds:us-
east-1:123456789012:cluster-snapshot:sample-cluster-snapshot ^
    --target-db-cluster-snapshot-identifier sample-cluster-snapshot-copy
```

La salida de esta operación será similar a lo que se indica a continuación.

```
{
```

```
    "DBClusterSnapshot": {
        "AvailabilityZones": [
            "us-east-1a",
            "us-east-1b",
            "us-east-1c"
        ],
        "DBClusterSnapshotIdentifier": "sample-cluster-snapshot-copy",
        "DBClusterIdentifier": "sample-cluster",
        "SnapshotCreateTime": "2020-04-29T16:45:51.239Z",
        "Engine": "docdb",
        "AllocatedStorage": 0,
        "Status": "copying",
        "Port": 0,
        "VpcId": "vpc-abc0123",
        "ClusterCreateTime": "2020-04-28T16:43:00.294Z",
        "MasterUsername": "master-user",
        "EngineVersion": "4.0.0",
        "LicenseModel": "docdb",
        "SnapshotType": "manual",
        "PercentProgress": 0,
        "StorageEncrypted": false,
        "DBClusterSnapshotArn": "arn:aws:rds:us-east-1:123456789012:cluster-
snapshot:sample-cluster-snapshot-copy",
        "SourceDBClusterSnapshotArn": "arn:aws:rds:us-east-1:123456789012:cluster-
snapshot:sample-cluster-snapshot",
    }
}
```

Example

Ejemplo 3: copiar una instantánea cifrada de un lado a otro Regiones de AWS

El siguiente AWS CLI ejemplo crea una copia de `sample-cluster-snapshot` de la región us-west-2 a la región us-east-1. Se llama a este comando en la región us-east-1.

Para Linux, macOS o Unix:

```
aws docdb copy-db-cluster-snapshot \
    --source-db-cluster-snapshot-identifier arn:aws:rds:us-
west-2:123456789012:cluster-snapshot:sample-cluster-snapshot \
    --target-db-cluster-snapshot-identifier sample-cluster-snapshot-copy \
    --source-region us-west-2 \
    --kms-key-id sample-us-east-1-key
```

Para Windows:

```
aws docdb copy-db-cluster-snapshot ^
    --source-db-cluster-snapshot-identifier arn:aws:rds:us-
west-2:123456789012:cluster-snapshot:sample-cluster-snapshot ^
    --target-db-cluster-snapshot-identifier sample-cluster-snapshot-copy ^
    --source-region us-west-2 ^
    --kms-key-id sample-us-east-1-key
```

La salida de esta operación será similar a lo que se indica a continuación.

```
{
    "DBClusterSnapshot": {
        "AvailabilityZones": [],
        "DBClusterSnapshotIdentifier": "sample-cluster-snapshot-copy",
        "DBClusterIdentifier": "sample-cluster",
        "SnapshotCreateTime": "2020-04-29T16:45:53.159Z",
        "Engine": "docdb",
        "AllocatedStorage": 0,
        "Status": "copying",
        "Port": 0,
        "ClusterCreateTime": "2020-04-28T16:43:07.129Z",
        "MasterUsername": "chimera",
        "EngineVersion": "4.0.0",
        "LicenseModel": "docdb",
        "SnapshotType": "manual",
        "PercentProgress": 0,
        "StorageEncrypted": true,
        "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/0846496a-
d48e-41c4-9353-86d8301d7e35",
        "DBClusterSnapshotArn": "arn:aws:rds:us-east-1:123456789012:cluster-
snapshot:sample-cluster-snapshot-copy",
        "SourceDBClusterSnapshotArn": "arn:aws:rds:us-west-2:123456789012:cluster-
snapshot:sample-cluster-snapshot",
    }
}
```

Example

Ejemplo 4: Copie una instantánea compartida sin cifrar de un lado a otro Regiones de AWS

El siguiente AWS CLI ejemplo, account -123456789012, crea una copia de una instantánea de clúster no cifrada `sample-cluster-snapshot` compartida por la cuenta, 999999999999

desde la región us-east-1 hasta la región us-west-2. Se llama a este comando en la región us-west-2. Para obtener más información sobre cómo compartir instantáneas, consulte Uso compartido de una instantánea.

Para Linux, macOS o Unix:

```
aws docdb copy-db-cluster-snapshot \
--region us-west-2 \
--source-db-cluster-snapshot-identifier arn:aws:rds:us-east-1:999999999999:cluster-snapshot:sample-cluster-snapshot \
--target-db-cluster-snapshot-identifier sample-cluster-snapshot-copy
```

Para Windows:

```
aws docdb copy-db-cluster-snapshot ^
--region us-west-2 ^
--source-db-cluster-snapshot-identifier arn:aws:rds:us-east-1:999999999999:cluster-snapshot:sample-cluster-snapshot ^
--target-db-cluster-snapshot-identifier sample-cluster-snapshot-copy
```

La salida de esta operación será similar a lo que se indica a continuación.

```
{
 "DBClusterSnapshots": [
 {
 "AvailabilityZones": [],
 "DBClusterSnapshotIdentifier": "sample-cluster-snapshot-copy",
 "DBClusterIdentifier": "sample-cluster",
 "SnapshotCreateTime": "2025-08-22T11:27:00.497000+00:00",
 "Engine": "docdb",
 "Status": "copying",
 "Port": 0,
 "ClusterCreateTime": "2024-07-02T16:44:50.246000+00:00",
 "MasterUsername": "master-user",
 "EngineVersion": "5.0.0",
 "SnapshotType": "manual",
 "PercentProgress": 0,
 "StorageEncrypted": false,
 "DBClusterSnapshotArn": "arn:aws:rds:us-west-2:123456789012:cluster-snapshot:sample-cluster-snapshot-copy",
 "SourceDBClusterSnapshotArn": "arn:aws:rds:us-east-1:999999999999:cluster-snapshot:sample-cluster-snapshot"
```

```
 }
 ]
}
```

Example

Ejemplo 5: Copie una instantánea compartida cifrada de un lado a otro Regiones de AWS

En el siguiente AWS CLI ejemplo, account: `123456789012` crea una copia de una instantánea de clúster cifrada `sample-cluster-snapshot` compartida por la cuenta, 999999999999 desde la región us-east-1 hasta la región us-west-2. La instantánea de destino está cifrada con una clave de KMS administrada por el cliente: `arn:aws:kms:us-west-2:123456789012:key/6c1f3264-1797-472b-ba37-03011e682d28`. Se llama a este comando en la región us-west-2. Para obtener más información sobre cómo compartir instantáneas, consulte Uso compartido de una instantánea.

Para Linux, macOS o Unix:

```
aws docdb copy-db-cluster-snapshot \
--region us-west-2 \
--source-db-cluster-snapshot-identifier arn:aws:rds:us-east-1:999999999999:cluster-snapshot:sample-cluster-snapshot \
--target-db-cluster-snapshot-identifier sample-cluster-snapshot-copy \
--kms-key-id arn:aws:kms:us-west-2:123456789012:key/6c1f3264-1797-472b-ba37-03011e682d28
```

Para Windows:

```
aws docdb copy-db-cluster-snapshot ^
--region us-west-2 ^
--source-db-cluster-snapshot-identifier arn:aws:rds:us-east-1:999999999999:cluster-snapshot:sample-cluster-snapshot ^
--target-db-cluster-snapshot-identifier sample-cluster-snapshot-copy ^
--kms-key-id arn:aws:kms:us-west-2:123456789012:key/6c1f3264-1797-472b-ba37-03011e682d28
```

La salida de esta operación será similar a lo que se indica a continuación.

```
{
 "DBClusterSnapshots": [
```

```
 {
 "AvailabilityZones": [],
 "DBClusterSnapshotIdentifier": "sample-cluster-snapshot-copy",
 "DBClusterIdentifier": "sample-cluster",
 "SnapshotCreateTime": "2025-08-22T11:27:00.497000+00:00",
 "Engine": "docdb",
 "Status": "copying",
 "Port": 0,
 "ClusterCreateTime": "2024-07-02T16:44:50.246000+00:00",
 "MasterUsername": "master-user",
 "EngineVersion": "5.0.0",
 "SnapshotType": "manual",
 "PercentProgress": 0,
 "StorageEncrypted": true,
 "KmsKeyId": "arn:aws:kms:us-west-2:123456789012:key/6c1f3264-1797-472b-
ba37-03011e682d28",
 "DBClusterSnapshotArn": "arn:aws:rds:us-west-2:123456789012:cluster-
snapshot:sample-cluster-snapshot-copy",
 "SourceDBClusterSnapshotArn": "arn:aws:rds:us-east-1:999999999999:cluster-
snapshot:sample-cluster-snapshot"
 }
 ]
}
```


> **Note**
>
> Para obtener más información acerca del cifrado de las copias de instantáneas, consulte Copia del cifrado de instantáneas de clúster.
> Para obtener más información sobre el cifrado en reposo, consulte Cifrado de datos en reposo de Amazon DocumentDB.

Uso compartido de instantáneas de clústeres de Amazon DocumentDB

Cuando utiliza Amazon DocumentDB, puede compartir una instantánea manual del clúster de las siguientes maneras:

- Al compartir una instantánea de un clúster manual, ya sea cifrada o no, AWS las cuentas autorizadas pueden copiar la instantánea.

- Al compartir una instantánea de un clúster manual, ya sea cifrada o no, AWS las cuentas autorizadas pueden restaurar directamente un clúster a partir de la instantánea, en lugar de tomar una copia del mismo y restaurarlo a partir de ahí.

> **Note**
>
> Para compartir una instantánea automatizada del clúster, cree una instantánea manual del clúster cuando copia la instantánea automatizada y, a continuación, comparta esa copia. Este proceso también se aplica a los recursos AWS generados por Backup.

Puede compartir una instantánea manual con hasta 20 personas más. Cuentas de AWS También puede compartir una instantánea manual sin cifrar como pública, lo que hace que esté disponible para todas las cuentas de . Si comparte una instantánea como pública, compruebe que no contiene información privada.

Al compartir instantáneas manuales con otras Cuentas de AWS personas y restaurar un clúster a partir de una instantánea compartida mediante la API AWS CLI o la API de Amazon DocumentDB, debe especificar el nombre de recurso de Amazon (ARN) de la instantánea compartida como identificador de la instantánea.

Cómo compartir una instantánea cifrada

Cuando se comparten instantáneas cifradas, se aplican las siguientes restricciones:

- No se pueden compartir instantáneas cifradas como públicas.
- No puede compartir una instantánea que se haya cifrado con la clave de AWS KMS cifrado predeterminada de la cuenta que compartió la instantánea.

Siga estos pasos para compartir instantáneas cifradas.

1. Comparta la clave de cifrado AWS Key Management Service (AWS KMS) que se utilizó para cifrar la instantánea con las cuentas a las que desee que puedan acceder a la instantánea.

   Puede compartir las claves de AWS KMS cifrado con otras AWS cuentas añadiendo las demás cuentas a la política de AWS KMS claves. Para obtener más información sobre la actualización de una política de claves, consulte Uso de políticas clave en AWS KMS en la Guía para AWS Key Management Service desarrolladores. Para ver un ejemplo de cómo crear una política de

claves, consulte Creación de una política de IAM para permitir la copia de la instantánea cifrada más adelante en este tema.

2. AWS CLI Utilícela, tal y como se muestra a continuación, para compartir la instantánea cifrada con las demás cuentas.

Permitir el acceso a una clave AWS KMS de cifrado

Para Cuenta de AWS que otra persona pueda copiar una instantánea cifrada compartida desde su cuenta, la cuenta con la que usted comparte la instantánea debe tener acceso a la AWS KMS clave que cifró la instantánea. Para permitir que otra cuenta acceda a una AWS KMS clave, actualice la política de claves de la AWS KMS clave con el ARN de la cuenta con la que comparte como principal en la política de AWS KMS claves. A continuación, permita la acción `kms:CreateGrant`.

Tras conceder a una cuenta acceso a la clave de AWS KMS cifrado, para copiar la instantánea cifrada, esa cuenta debe crear un usuario AWS Identity and Access Management (IAM) si aún no lo tiene. Además, esa cuenta también debe adjuntar una política de IAM a ese usuario de IAM que le permita copiar una instantánea cifrada con su clave. AWS KMS La cuenta debe ser un usuario de IAM y no puede ser una Cuenta de AWS identidad raíz debido a AWS KMS restricciones de seguridad.

En el siguiente ejemplo de política de claves, el usuario 123451234512 es el propietario de la clave de cifrado. AWS KMS El usuario 123456789012 es la cuenta con la que se comparte la clave. Esta política de claves actualizada permite a la cuenta acceder a la clave. AWS KMS Para ello, incluye el ARN de la Cuenta de AWS identidad raíz del usuario 123456789012 como principal de la política y permite la acción. `kms:CreateGrant`

JSON

```
{
    "Id": "key-policy-1",
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "Allow use of the key",
            "Effect": "Allow",
            "Principal": {"AWS": [
                "arn:aws:iam::123451234512:user/KeyUser",
                "arn:aws:iam::123456789012:root"
            ]},
```

```
            "Action": [
                "kms:CreateGrant",
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": "*"},
            {
            "Sid": "Allow attachment of persistent resources",
            "Effect": "Allow",
            "Principal": {"AWS": [
                "arn:aws:iam::123451234512:user/KeyUser",
                "arn:aws:iam::123456789012:root"
            ]},
            "Action": [
                "kms:CreateGrant",
                "kms:ListGrants",
                "kms:RevokeGrant"
            ],
            "Resource": "*",
            "Condition": {"Bool": {"kms:GrantIsForAWSResource": true}}
        }
    ]
}
```

Creación de una política de IAM para permitir la copia de la instantánea cifrada

Cuando una persona externa Cuenta de AWS tenga acceso a tu AWS KMS clave, el propietario de esa cuenta puede crear una política que permita a un usuario de IAM creado para la cuenta copiar una instantánea cifrada que esté cifrada con esa clave. AWS KMS

En el siguiente ejemplo, se muestra una política que se puede adjuntar a un usuario de IAM para Cuenta de AWS 123456789012. La política permite al usuario de IAM copiar una instantánea compartida de la cuenta 123451234512 que se haya cifrado con la clave AWS KMS en `c989c1dd-a3f2-4a5d-8d96-e793d082ab26` la región us-west-2.

JSON

```
{
```

```
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowUseOfTheKey",
            "Effect": "Allow",
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey",
                "kms:CreateGrant",
                "kms:RetireGrant"
            ],
            "Resource": ["arn:aws:kms:us-west-2:123451234512:key/c989c1dd-
a3f2-4a5d-8d96-e793d082ab26"]
        },
        {
            "Sid": "AllowAttachmentOfPersistentResources",
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant",
                "kms:ListGrants",
                "kms:RevokeGrant"
            ],
            "Resource": ["arn:aws:kms:us-west-2:123451234512:key/c989c1dd-
a3f2-4a5d-8d96-e793d082ab26"],
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
        }
    ]
}
```

Para obtener información detallada sobre cómo actualizar una política de claves, consulte Uso de políticas de claves en AWS KMS de la Guía para desarrolladores de AWS Key Management Service .

Uso compartido de una instantánea

Puede compartir una instantánea manual de un clúster de Amazon DocumentDB (o una copia de una instantánea automática) mediante: Consola de administración de AWS AWS CLI

Using the Consola de administración de AWS

Para compartir una instantánea mediante el Consola de administración de AWS, complete los siguientes pasos:

1. Inicie sesión en y abra la Consola de administración de AWS consola de Amazon DocumentDB en https://console.aws.amazon.com /docdb.
2. En el panel de navegación, elija Snapshots (Instantáneas).
3. Seleccione la instantánea manual que desea compartir.
4. En el menú desplegable Acciones, elija Compartir.
5. Elija una de las siguientes opciones para Visibilidad de instantánea de base de datos.

   - Si la fuente no está cifrada, seleccione Pública para permitir que todas las AWS cuentas restauren un clúster a partir de la instantánea manual. O bien, elige Privado para permitir que solo AWS las cuentas que especifiques restauren un clúster a partir de la instantánea manual.

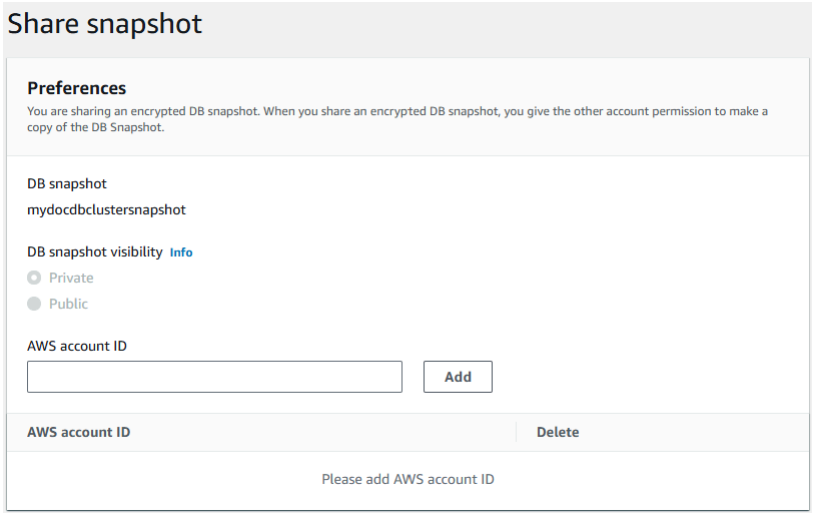
     > **Warning**
     >
     > Si establece la visibilidad de la instantánea de base de datos en Pública, todas AWS las cuentas pueden restaurar un clúster a partir de la instantánea manual y tener acceso a sus datos. No comparta como Pública ninguna instantánea manual del clúster que contenga información confidencial.

   - Si el original está cifrado, DB Snapshot Visibility (Visibilidad de instantánea de base de datos) se establece en Private (Privada), ya que las instantáneas cifradas no se pueden compartir como públicas.

     > **Note**
     >
     > Las instantáneas que se hayan cifrado con la configuración predeterminada no se AWS KMS key pueden compartir.

6. En el AWS campo ID de AWS cuenta, introduce el identificador de la cuenta a la que quieras permitir que restaure un clúster a partir de la instantánea manual y, a continuación, selecciona Añadir. Repite este procedimiento para incluir identificadores de AWS cuenta adicionales, hasta 20 AWS cuentas.

   Si cometes un error al añadir un identificador de AWS cuenta a la lista de cuentas permitidas, puedes eliminarlo de la lista seleccionando Eliminar a la derecha del identificador de AWS cuenta incorrecto.



7. Una vez que haya añadido los identificadores de todas las AWS cuentas que desee permitir que se restablezca la instantánea manual, pulse Guardar para guardar los cambios.

Using the AWS CLI

Para compartir una instantánea mediante AWS CLI, utilice la operación Amazon DocumentDB. `modify-db-snapshot-attribute` Utilice el `--values-to-add` parámetro para añadir una lista de los IDs Cuentas de AWS que están autorizados a restaurar la instantánea manual.

El siguiente ejemplo permite que dos Cuenta de AWS identificadores, 123451234512 y 123456789012, restauren la instantánea nombrada. `manual-snapshot1` También se elimina el valor del atributo `all` para marcar la instantánea como privada.

Para Linux, macOS o Unix:

```
aws docdb modify-db-cluster-snapshot-attribute \
    --db-cluster-snapshot-identifier sample-cluster-snapshot \
    --attribute-name restore \
    --values-to-add '["123451234512","123456789012"]'
```

Para Windows:

```
aws docdb modify-db-cluster-snapshot-attribute ^
    --db-cluster-snapshot-identifier sample-cluster-snapshot ^
    --attribute-name restore ^
    --values-to-add '["123451234512","123456789012"]'
```

La salida de esta operación será similar a lo que se indica a continuación.

```
{
    "DBClusterSnapshotAttributesResult": {
        "DBClusterSnapshotIdentifier": "sample-cluster-snapshot",
        "DBClusterSnapshotAttributes": [
            {
                "AttributeName": "restore",
                "AttributeValues": [
                    "123451234512",
                    "123456789012"
                ]
            }
        ]
    }
}
```

Para eliminar un Cuenta de AWS identificador de la lista, utilice el parámetro. `--values-to-remove` El siguiente ejemplo impide que el Cuenta de AWS ID 123456789012 restaure la instantánea.

Para Linux, macOS o Unix:

```
aws docdb modify-db-cluster-snapshot-attribute \
    --db-cluster-snapshot-identifier sample-cluster-snapshot \
    --attribute-name restore \
    --values-to-remove '["123456789012"]'
```

Para Windows:

```
aws docdb modify-db-cluster-snapshot-attribute ^
    --db-cluster-snapshot-identifier sample-cluster-snapshot ^
    --attribute-name restore ^
    --values-to-remove '["123456789012"]'
```

La salida de esta operación será similar a lo que se indica a continuación.

```
{
    "DBClusterSnapshotAttributesResult": {
        "DBClusterSnapshotIdentifier": "sample-cluster-snapshot",
        "DBClusterSnapshotAttributes": [
            {
                "AttributeName": "restore",
                "AttributeValues": [
                    "123451234512"
                ]
            }
        ]
    }
}
```

Restauración de una instantánea del clúster

Amazon DocumentDB (compatible con MongoDB) crea una instantánea del clúster del volumen de almacenamiento. Puede crear un clúster nuevo restaurándolo a partir de una instantánea de clúster. Al restaurar el clúster, debe indicar el nombre de la instantánea del clúster desde la que se realiza la restauración y un nombre para el clúster nuevo que se crea con la operación de restauración. No es posible restaurar desde una instantánea a un clúster existente, ya que al realizar la restauración se crea un clúster nuevo.

Al restaurar un clúster a partir de una instantánea de clúster:

- Esta acción solo restaura el clúster, no las instancias de ese clúster. Debe invocar la acción `create-db-instance` para crear instancias para el clúster restaurado, especificando el identificador de dicho clúster restaurado en `--db-cluster-identifier`. Solo es posible crear las instancias después de que el clúster esté disponible.
- No se puede restaurar una instantánea cifrada en un clúster sin cifrar. Sin embargo, puede restaurar una instantánea no cifrada en un clúster cifrado especificando la clave. AWS KMS
- Para restaurar un clúster a partir de una instantánea cifrada, debe tener acceso a la AWS KMS clave.

> **Note**
>
> No puede restaurar un clúster 3.6 a uno 4.0, pero puede migrar de una versión de clúster a otra. Para obtener más información, consulte Migración a Amazon DocumentDB.

Using the Consola de administración de AWS

El procedimiento siguiente muestra cómo restaurar un clúster de Amazon DocumentDB a partir de una instantánea de clúster mediante la consola de administración de Amazon DocumentDB.

1. Inicie sesión en y abra la Consola de administración de AWS consola de Amazon DocumentDB en https://console.aws.amazon.com /docdb.
2. En el panel de navegación, elija Snapshots (Instantáneas) y, a continuación, elija el botón situado a la izquierda de la instantánea que desea utilizar para restaurar un clúster.

   > **Tip**
   >
   > Si no ve el panel de navegación del lado izquierdo de la pantalla, seleccione el icono de menú
   > (≡)
   > en la esquina superior izquierda de la página.

3. En el menú Actions (Acciones), seleccione Restore (Restaurar).
4. En la página Restore snapshot (Restaurar instantánea), rellene la sección Configuration (Configuración).

   a. Identificador de clúster: nombre del nuevo clúster. Puede aceptar el nombre facilitado por Amazon DocumentDB o escribir el nombre que prefiera. El DBsupplied nombre del documento de Amazon tiene el formato de `docdb-` más una marca de tiempo UTC; por ejemplo,. `docdb-yyyy-mm-dd-hh-mm-ss`

   b. Clase de instancia: clase de instancia del nuevo clúster. Puede aceptar la clase de instancia predeterminada o elegir una en la lista desplegable.

   c. Número de instancias: número de instancias que desea crear con este clúster. Puede aceptar el valor predeterminado de 3 instancias (1 réplica principal read/write y 2 réplicas de solo lectura) o elegir el número de instancias de la lista desplegable.

5. En Configuración del almacenamiento en clúster, elija una opción de almacenamiento.

> **Note**
>
> La configuración de almacenamiento Amazon DocumentDB optimizado para E/S solo está disponible en la versión 5.0 del motor de Amazon DocumentDB.

6. Si está satisfecho con la configuración del clúster, elija Restore cluster (Restaurar clúster) y espere mientras el clúster se restaura.
7. Si prefiere cambiar algunas configuraciones, como especificar un grupo de seguridad o Amazon VPC no predeterminados, elija Mostrar configuración avanzada en la esquina inferior izquierda de la página y, después, continúe con los pasos siguientes.

   a. Rellene la sección Network settings (Configuración de red).

      - Nube privada virtual (VPC): acepte la VPC actual o elija una de la lista desplegable.
      - Grupo de subredes: acepte el grupo de subredes `default` o elija uno de la lista desplegable.
      - Grupos de seguridad de la VPC: acepte el grupo de seguridad `default (VPC)` o elija uno de la lista.

   b. Rellene la sección Cluster options (Opciones de clúster).

      - Puerto de base de datos: acepte el puerto predeterminado, `27017`, o utilice la flecha hacia arriba o hacia abajo para establecer el puerto que desea utilizar para las conexiones de las aplicaciones.

   c. Rellene la sección Encryption (Cifrado).

      - Cifrado en reposo: si la instantánea está cifrada, estas opciones no están disponibles. Si no está cifrada, puede elegir una de las opciones siguientes:
        - Para cifrar todos los datos del clúster, selecciona Activar. encryption-at-rest Si elige esta opción, debe designar una clave de KMS.
        - Para no cifrar los datos del clúster, selecciona Desactivar. encryption-at-rest Si elige esta opción, habrá terminado con la sección de cifrado.
      - AWS KMS Clave: elija una de las siguientes opciones de la lista desplegable:
        - (predeterminado) aws/rds: el número de cuenta y el identificador AWS KMS clave aparecen siguiendo esta opción.

- Clave gestionada por el cliente: esta opción solo está disponible si ha creado una clave de cifrado de IAM en la consola (IAM). AWS Identity and Access Management Puede elegir la clave que desea utilizar para cifrar el clúster.
- Introduzca un ARN clave: en el cuadro ARN, introduzca el nombre del recurso de Amazon (ARN) de su clave. AWS KMS El formato del ARN es el siguiente: `arn:aws:kms:<region>:<accountID>:key/<key-id>`.

d. Rellene la sección Log exports (Exportaciones de registros).

- Seleccione los tipos de registro en los que desea publicar CloudWatch: elija una de las siguientes opciones:
  - Activado: permite que el clúster exporte los registros de DDL a Amazon CloudWatch Logs.
  - Desactivado: impide que el clúster exporte los registros de DDL a Amazon CloudWatch Logs. La opción Disabled (Deshabilitado) es la predeterminada.
- Rol de IAM: en la lista, seleccione Rol vinculado al servicio RDS.

e. Complete la sección Tags (Etiquetas).

- Agregar etiqueta: en el cuadro Clave, escriba el nombre de la etiqueta del clúster. En el cuadro Value (Valor), si lo desea, escriba el valor de la etiqueta. Las etiquetas se utilizan con las políticas AWS Identity and Access Management (de IAM) para administrar el acceso a los recursos de Amazon DocumentDB y controlar qué acciones se pueden aplicar a los recursos.

f. Complete la sección Deletion protection (Protección contra la eliminación).

- Habilitar la protección contra la eliminación: protege el clúster para que no se pueda eliminar accidentalmente. Cuando esta opción está habilitada, no se puede eliminar el clúster.

8. Elija Restore cluster (Restaurar clúster).

Using the AWS CLI

Para restaurar un clúster a partir de una instantánea mediante la AWS CLI, utilice la `restore-db-cluster-from-snapshot` operación con los siguientes parámetros. Para obtener más información, consulte RestoreDBClusterFromSnapshot.

- **`--db-cluster-identifier`**: obligatorio. Escriba el nombre del clúster que va a crear la operación. No puede existir un clúster con este nombre antes de esta operación.

  Restricciones en cuanto a la nomenclatura de los clústeres:

  - Debe tener [1-63] letras, números o guiones.
  - El primer carácter debe ser una letra.
  - No puede terminar con un guion ni contener dos guiones consecutivos.
  - Debe ser único para todos los clústeres de Amazon RDS, Neptune y Amazon DocumentDB por región. Cuenta de AWS
- **`--snapshot-identifier`**: obligatorio. El nombre de la instantánea desde la que se va a restaurar. Debe existir una instantánea con este nombre y tener el estado disponible.
- **`--engine`**: obligatorio. Debe ser `docdb`.
- **`--storage-type standard | iopt1`**: opcional. Predeterminado: `standard`.
- **`--kms-key-id`**— Opcional. El ARN del identificador de AWS KMS clave que se utilizará al restaurar una instantánea cifrada o al cifrar un clúster al restaurar desde una instantánea no cifrada. Al proporcionar el ID de AWS KMS clave, el clúster restaurado se cifra con la AWS KMS clave, esté cifrada o no la instantánea.

  El formato de `--kms-key-id` es `arn:aws:kms:<region>:<accountID>:key/<key-id>`. Si no se especifica un valor para el parámetro `--kms-key-id`, ocurre lo siguiente:

  - Si la instantánea `--snapshot-identifier` está cifrada, el clúster restaurado se cifra con la misma AWS KMS clave que se utilizó para cifrar la instantánea.
  - Si la instantánea indicada con `--snapshot-identifier` no está cifrada, el clúster restaurado no está cifrado.

Para Linux, macOS o Unix:

```
aws docdb restore-db-cluster-from-snapshot \
    --db-cluster-identifier sample-cluster-restore \
    --snapshot-identifier sample-cluster-snapshot \
    --engine docdb \
    --kms-key-id arn:aws:kms:us-east-1:123456789012:key/SAMPLE-KMS-KEY-ID
```

Para Windows:

```
aws docdb restore-db-cluster-from-snapshot ^
```

```
    --db-cluster-identifier sample-cluster-restore ^
    --snapshot-identifier sample-cluster-snapshot ^
    --engine docdb ^
    --kms-key-id arn:aws:kms:us-east-1:123456789012:key/SAMPLE-KMS-KEY-ID
```

La salida de esta operación será similar a lo que se indica a continuación.

```
{
    "DBCluster": {
        "AvailabilityZones": [
            "us-east-1c",
            "us-east-1b",
            "us-east-1a"
        ],
        "BackupRetentionPeriod": 1,
        "DBClusterIdentifier": "sample-cluster-restore",
        "DBClusterParameterGroup": "default.docdb4.0",
        "DBSubnetGroup": "default",
        "Status": "creating",
        "Endpoint": "sample-cluster-restore.cluster-node.us-
east-1.docdb.amazonaws.com",
        "ReaderEndpoint": "sample-cluster-restore.cluster-node.us-
east-1.docdb.amazonaws.com",
        "MultiAZ": false,
        "Engine": "docdb",
        "EngineVersion": "4.0.0",
        "Port": 27017,
        "MasterUsername": "<master-user>",
        "PreferredBackupWindow": "02:00-02:30",
        "PreferredMaintenanceWindow": "tue:09:50-tue:10:20",
        "DBClusterMembers": [],
        "VpcSecurityGroups": [
            {
                "VpcSecurityGroupId": "sg-abcdefgh",
                "Status": "active"
            }
        ],
        "HostedZoneId": "ABCDEFGHIJKLM",
        "StorageEncrypted": true,
        "KmsKeyId": "arn:aws:kms:us-east-1:<accountID>:key/<sample-key-id>",
        "DbClusterResourceId": "cluster-ABCDEFGHIJKLMNOPQRSTUVWXYZ",
        "DBClusterArn": "arn:aws:rds:us-east-1:<accountID>:cluster:sample-cluster-
restore",
```

```
        "AssociatedRoles": [],
        "ClusterCreateTime": "2020-04-01T01:43:40.871Z",
        "DeletionProtection": true
    }
}
```

Una vez que el estado del clúster sea disponible, cree al menos una instancia para el clúster.

Para Linux, macOS o Unix:

```
aws docdb create-db-instance \
    --db-cluster-identifier sample-cluster-restore  \
    --db-instance-identifier sample-cluster-restore-instance \
    --availability-zone us-east-1b \
    --promotion-tier 2 \
    --db-instance-class db.r5.large \
    --engine docdb
```

Para Windows:

```
aws docdb create-db-instance ^
    --db-cluster-identifier sample-cluster-restore  ^
    --db-instance-identifier sample-cluster-restore-instance ^
    --availability-zone us-east-1b ^
    --promotion-tier 2 ^
    --db-instance-class db.r5.large ^
    --engine docdb
```

La salida de esta operación será similar a lo que se indica a continuación.

```
{
    "DBInstance": {
        "DBInstanceIdentifier": "sample-cluster-restore-instance",
        "DBInstanceClass": "db.r5.large",
        "Engine": "docdb",
        "DBInstanceStatus": "creating",
        "PreferredBackupWindow": "02:00-02:30",
        "BackupRetentionPeriod": 1,
        "VpcSecurityGroups": [
            {
                "VpcSecurityGroupId": "sg-abcdefgh",
                "Status": "active"
```

```
            }
        ],
        "AvailabilityZone": "us-west-2b",
        "DBSubnetGroup": {
            "DBSubnetGroupName": "default",
            "DBSubnetGroupDescription": "default",
            "VpcId": "vpc-6242c31a",
            "SubnetGroupStatus": "Complete",
            "Subnets": [
                {
                    "SubnetIdentifier": "subnet-abcdefgh",
                    "SubnetAvailabilityZone": {
                        "Name": "us-west-2a"
                    },
                    "SubnetStatus": "Active"
                },
                {
                    ...
                }
            ]
        },
        "PreferredMaintenanceWindow": "fri:09:43-fri:10:13",
        "PendingModifiedValues": {},
        "EngineVersion": "4.0.0",
        "AutoMinorVersionUpgrade": true,
        "PubliclyAccessible": false,
        "DBClusterIdentifier": "sample-cluster-restore",
        "StorageEncrypted": true,
        "KmsKeyId": "arn:aws:kms:us-east-1:<accountID>:key/<sample-key-id>",
        "DbiResourceId": "db-ABCDEFGHIJKLMNOPQRSTUVWXYZ",
        "CACertificateIdentifier": "rds-ca-2019",
        "PromotionTier": 2,
        "DBInstanceArn": "arn:aws:rds:us-east-1:<accountID>:db:sample-cluster-
restore-instance"
    }
}
```

Restauración a un momento dado

Puede restaurar un clúster en cualquier momento que se encuentre dentro del período de retención de la copia de seguridad del clúster mediante Consola de administración de AWS o AWS Command Line Interface (AWS CLI).

> **Note**
>
> No puedes realizar una point-in-time restauración de un clúster 3.6 a uno 4.0, pero puedes migrar de una versión de clúster a otra. Para obtener más información, consulte Migración a Amazon DocumentDB.

Tenga en cuenta las siguientes consideraciones al restaurar un clúster de base de datos a un momento dado.

- El nuevo clúster se crea con la misma configuración que el clúster de origen, con la salvedad de que el nuevo clúster se crea con el grupo de parámetros predeterminado. Para establecer el nuevo grupo de parámetros de clúster en el grupo de parámetros de clúster de origen, modifique el clúster en cuanto esté disponible. Para obtener más información acerca de la modificación de un clúster, consulte Modificación de un clúster de Amazon DocumentDB.

Using the Consola de administración de AWS

Para restaurar un clúster point-in-time dentro de su período de retención de copias de seguridad, complete lo siguiente mediante el Consola de administración de AWS.

1. Inicie sesión en y abra la Consola de administración de AWS consola de Amazon DocumentDB en https://console.aws.amazon.com /docdb.
2. En el panel de navegación, seleccione Clusters (Clústeres). En la lista de clústeres, elija el botón situado a la izquierda del clúster que desee restaurar.

   > **Tip**
   >
   > Si no ve el panel de navegación del lado izquierdo de la pantalla, seleccione el icono de menú
   > (≡)
   > en la esquina superior izquierda de la página.

3. En el menú Actions (Acciones), seleccione Restore to point in time (Restaurar a un momento dado).
4. Rellene la sección Restore time (Hora de restauración), en la que se especifican la fecha y la hora a la que restaurar.

a. Fecha de restauración: elija o introduzca una fecha que esté entre la hora de restauración más temprana y la hora de restauración más reciente.

b. Hora de restauración: elija o introduzca la hora, el minuto y los segundos que están entre la hora de restauración más temprana y la hora de restauración más reciente.

5. Rellene la sección Configuration (Configuración).

a. Identificador de clúster: acepte el identificador predeterminado o introduzca otro identificador de su elección.

Restricciones en cuanto a la nomenclatura de los clústeres:

- Debe tener [1-63] letras, números o guiones.
- El primer carácter debe ser una letra.
- No puede terminar con un guion ni contener dos guiones consecutivos.
- Debe ser único para todos los clústeres de Amazon RDS, Neptune y Amazon DocumentDB por región. Cuenta de AWS

b. Clase de instancia: en la lista desplegable, elija la clase de instancia que desea utilizar para las instancias del clúster.

c. Número de instancias: en la lista desplegable, elija el número de instancias que desee crear cuando se restaure el clúster.

6. En Configuración del almacenamiento en clúster, elija una opción de almacenamiento.

> **Note**
>
> La configuración de almacenamiento Amazon DocumentDB optimizado para E/S solo está disponible en la versión 5.0 del motor de Amazon DocumentDB.

7. Opcional. Para configurar los ajustes de red y las opciones de clúster y para habilitar las exportaciones de registros, elija Show advanced settings (Mostrar configuración avanzada) y complete dichas secciones. De lo contrario, continúe en el siguiente paso.

- Network settings (Configuración de red)
  1. Nube privada virtual (VPC): en la lista desplegable, elija la VPC que quiera usar para este clúster.
  2. Grupo de subredes: en la lista desplegable, elija el grupo de subredes para este clúster.

3. Grupos de seguridad de la VPC: en la lista desplegable, elija el grupo de seguridad de la VPC para este clúster.

- Cluster options (Opciones de clúster)
  1. Puerto: acepte el puerto predeterminado (27017) o utilice las flechas hacia arriba y abajo para establecer el puerto de comunicación con este clúster.

- Log exports (Exportaciones de registros)
  1. Registros de auditoría: seleccione esta opción para habilitar la exportación de registros de auditoría a Amazon CloudWatch Logs. Si selecciona esta opción, debe habilitar `audit_logs` en el grupo personalizado de parámetros de clúster. Para obtener más información, consulte Auditoría de eventos de Amazon DocumentDB.
  2. Registros del generador de perfiles: seleccione esta opción para permitir la exportación de los registros del generador de perfiles de operaciones a Amazon CloudWatch Logs. Si selecciona esta opción, también debe modificar los siguientes parámetros del grupo personalizado de parámetros del clúster:
     - `profiler`: se establece en `enabled`.
     - `profiler_threshold_ms`: se establece en un valor `[0-INT_MAX]` para definir el umbral para las operaciones de creación de perfiles.
     - `profiler_sampling_rate`: se establece en un valor `[0.0-1.0]` para definir el porcentaje de operaciones lentas en el perfil.

     Para obtener más información, consulte Creación de perfiles de operaciones en Amazon DocumentDB.
  3. Registros del generador de perfiles: exporta los registros del generador de perfiles a Amazon CloudWatch
  4. Rol de IAM: en la lista desplegable, seleccione Rol vinculado al servicio RDS.
- Etiquetas
  1. Agregar etiqueta: en el cuadro Clave, escriba el nombre de la etiqueta del clúster. En el cuadro Value (Valor), si lo desea, escriba el valor de la etiqueta. Las etiquetas se utilizan con las políticas de AWS Identity and Access Management (IAM) para administrar el acceso a los recursos de Amazon DocumentDB y para controlar qué acciones se pueden aplicar a los recursos.

- Protección contra eliminación

  1. Habilitar la protección contra la eliminación: protege el clúster para que no se pueda eliminar accidentalmente. Cuando esta opción está habilitada, no se puede eliminar el clúster.

8. Para restaurar el clúster, elija Create cluster (Crear clúster). También puede elegir Cancel (Cancelar) para cancelar la operación.

Using the AWS CLI

Para restaurar un clúster a un momento dado mediante el periodo de retención de copia de seguridad de la instantánea, utilice la operación `restore-db-cluster-to-point-in-time` con los siguientes parámetros.

- **`--db-cluster-identifier`**: obligatorio. El nombre del nuevo clúster que se va a crear. Este clúster no puede existir antes de la operación. El valor del parámetro debe cumplir las siguientes restricciones.

  Restricciones en cuanto a la nomenclatura de los clústeres:

  - Debe tener [1-63] letras, números o guiones.
  - El primer carácter debe ser una letra.
  - No puede terminar con un guion ni contener dos guiones consecutivos.
  - Debe ser único para todos los clústeres de Amazon RDS, Neptune y Amazon DocumentDB por región. Cuenta de AWS

- **`--restore-to-time`**: la fecha y la hora UTC en que se va a restaurar el clúster. Por ejemplo, `2018-06-07T23:45:00Z`.

  Restricciones de tiempo:

  - Debe ser anterior a la última hora restaurable del clúster.
  - Debe especificarse si no se proporciona el parámetro `--use-latest-restorable-time`.
  - No se puede especificar si el parámetro `--use-latest-restorable-time` es `true`.
  - No se puede especificar si el valor del parámetro `--restore-type` es `copy-on-write`.

- **`--source-db-cluster-identifier`**: el nombre del clúster de origen desde el que se va a restaurar. Este clúster debe existir y estar disponible.

- **`--use-latest-restorable-time`** o **`--no-use-latest-restorable-time`**: si se va a restaurar a la hora más reciente de la copia de seguridad restaurable. No se puede especificar si se proporciona el parámetro `--restore-to-time`.
- **`--storage-type standard | iopt1`**: opcional. Predeterminado: `standard`.

La AWS CLI operación `restore-db-cluster-to-point-in-time` solo restaura el clúster, no las instancias de ese clúster. Debe invocar la operación `create-db-instance` para crear instancias para el clúster restaurado, especificando el identificador de dicho clúster restaurado en `--db-cluster-identifier`. Solo puede crear instancias después de que se haya completado la operación `restore-db-cluster-to-point-in-time` y de que el clúster restaurado esté disponible.

Example

En el siguiente ejemplo, `sample-cluster-restored` se crea a partir de la instantánea `sample-cluster-snapshot` tomando el último momento que se puede restaurar.

Para Linux, macOS o Unix:

```
aws docdb restore-db-cluster-to-point-in-time \
    --db-cluster-identifier sample-cluster-restored \
    --source-db-cluster-identifier sample-cluster-snapshot \
    --use-latest-restorable-time
```

Para Windows:

```
aws docdb restore-db-cluster-to-point-in-time ^
    --db-cluster-identifier sample-cluster-restored ^
    --source-db-cluster-identifier sample-cluster-snapshot ^
    --use-latest-restorable-time
```

Example

En el siguiente ejemplo, `sample-cluster-restored` se crea a partir de la instantánea `sample-cluster-snapshot` en el punto en el que estaba a las 03:15 del 11 de diciembre de 2018 (UTC), que está dentro del periodo de retención de copia de seguridad de `sample-cluster`.

Para Linux, macOS o Unix:

```
aws docdb restore-db-cluster-to-point-in-time \
    --db-cluster-identifier sample-cluster-restore \
    --source-db-cluster-identifier sample-cluster \
    --restore-to-time 2020-05-12T03:15:00Z
```

Para Windows:

```
aws docdb restore-db-cluster-to-point-in-time ^
    --db-cluster-identifier sample-cluster-restore ^
    --source-db-cluster-identifier sample-cluster ^
    --restore-to-time 2020-05-12T03:15:00Z
```

La salida de esta operación será similar a lo que se indica a continuación.

```
{
    "DBCluster": {
        "AvailabilityZones": [
            "us-east-1c",
            "us-west-2b",
            "us-west-2a"
        ],
        "BackupRetentionPeriod": 1,
        "DBClusterIdentifier": "sample-cluster-restored",
        "DBClusterParameterGroup": "sample-parameter-group",
        "DBSubnetGroup": "default",
        "Status": "creating",
        "Endpoint": "sample-cluster-restored.node.us-east-1.docdb.amazonaws.com",
        "ReaderEndpoint": "sample-cluster-restored.node.us-
east-1.docdb.amazonaws.com",
        "MultiAZ": false,
        "Engine": "docdb",
        "EngineVersion": "4.0.0",
        "Port": 27017,
        "MasterUsername": "master-user",
        "PreferredBackupWindow": "02:00-02:30",
        "PreferredMaintenanceWindow": "tue:09:50-tue:10:20",
        "DBClusterMembers": [],
        "VpcSecurityGroups": [
            {
                "VpcSecurityGroupId": "sg-abc0123",
                "Status": "active"
            }
```

```
        ],
        "HostedZoneId": "ABCDEFGHIJKLM",
        "StorageEncrypted": true,
        "KmsKeyId": "arn:aws:kms:us-east-1:<accountID^>:key/sample-key",
        "DbClusterResourceId": "cluster-ABCDEFGHIJKLMNOPQRSTUVWXYZ",
        "DBClusterArn": "arn:aws:rds:us-east-1:<accountID>:cluster:sample-cluster-
restored",
        "AssociatedRoles": [],
        "ClusterCreateTime": "2020-04-24T20:14:36.713Z",
        "DeletionProtection": false
    }
}
```

Eliminación de una instantánea del clúster

Una instantánea manual es una copia de seguridad completa que se elimina solo cuando se elimina manualmente mediante la tecla Consola de administración de AWS o AWS CLI. No se puede eliminar manualmente una instantánea automática, porque las instantáneas automáticas solo se eliminan cuando finaliza el período de retención o cuando elimina el clúster de la instantánea.

Using the Consola de administración de AWS

Para eliminar una instantánea de clúster manual mediante el Consola de administración de AWS, complete los siguientes pasos.

1. Inicie sesión en y abra la Consola de administración de AWS consola de Amazon DocumentDB en https://console.aws.amazon.com /docdb.
2. En el panel de navegación, elija Snapshots (Instantáneas).

   > **Tip**
   >
   > Si no ve el panel de navegación del lado izquierdo de la pantalla, seleccione el icono de menú
   > (≡)
   > en la esquina superior izquierda de la página.

3. En la lista de instantáneas, elija el botón situado a la izquierda de la instantánea que desea eliminar. El tipo de la instantánea debe ser manual.

1. Puede verificar que el tipo de instantánea es manual comprobando si aparece enumerado como `manual` o `automatic` en la columna Tipo.

4. En el menú Actions (Acciones), elija Delete (Eliminar). Si la opción Delete (Eliminar) no está disponible, lo más probable es que haya elegido una instantánea automática.
5. En la pantalla de confirmación de eliminación, para eliminar la instantánea, seleccione Delete (Eliminar). Para conservar la instantánea, elija Cancel (Cancelar).

Using the AWS CLI

Una instantánea manual del clúster de Amazon DocumentDB es una copia de seguridad completa que puede eliminar manualmente mediante la AWS CLI. No puede eliminar manualmente una instantánea automática.

Para eliminar una instantánea de clúster manual mediante el AWS CLI, utilice la `delete-db-cluster-snapshot` operación con los siguientes parámetros.

Parameters

- **`--db-cluster-snapshot-identifier`**: obligatorio. El nombre de la instantánea manual que se va a eliminar.

En el siguiente ejemplo se elimina la instantánea `sample-cluster-snapshot` del clúster:

Para Linux, macOS o Unix:

```
aws docdb delete-db-cluster-snapshot \
    --db-cluster-snapshot-identifier sample-cluster-snapshot
```

Para Windows:

```
aws docdb delete-db-cluster-snapshot ^
    --db-cluster-snapshot-identifier sample-cluster-snapshot
```

En la salida de esta operación, se muestran los detalles de la instantánea de clúster que ha eliminado.

Administración de recursos de Amazon DocumentDB

En estas secciones se describen los distintos componentes y sus tareas relacionadas para administrar la implementación de Amazon DocumentDB (con compatibilidad con MongoDB).

Temas

- Información general sobre las tareas operativas de Amazon DocumentDB
- Información general de los clústeres globales de Amazon DocumentDB
- Administración de clústeres de Amazon DocumentDB
- Administración de instancias de Amazon DocumentDB
- Administración de grupos de subredes de Amazon DocumentDB
- Alta disponibilidad y replicación de Amazon DocumentDB
- Administración de índices de Amazon DocumentDB
- Gestión de la compresión de documentos a nivel de colección
- Administración de la compresión basada en diccionarios en Amazon DocumentDB 8.0
- Administración de eventos de Amazon DocumentDB
- Elección de regiones y zonas de disponibilidad
- Administración de los grupos de parámetros de clúster de Amazon DocumentDB
- Descripción de los puntos de conexión de Amazon DocumentDB
- Descripción de los nombres de recursos de Amazon DocumentDB () ARNs
- Etiquetado de recursos de Amazon DocumentDB
- Mantenimiento de Amazon DocumentDB
- Descripción de los roles vinculados a servicios
- Uso de flujos de cambios con Amazon DocumentDB
- Uso de la intercalación en Amazon DocumentDB 8.0
- Uso de vistas en Amazon DocumentDB 8.0
- Uso de AWS Lambda con flujos de cambios

Información general sobre las tareas operativas de Amazon DocumentDB

En esta sección se explican las tareas operativas de un clúster de Amazon DocumentDB y cómo llevar a cabo estas tareas mediante la AWS CLI.

Temas

- Agregación de una réplica a un clúster de Amazon DocumentDB
- Descripción de clústeres e instancias
- Creación de una instantánea de un clúster
- Restauración a partir de una instantánea
- Eliminación de una instancia de un clúster
- Eliminación de un clúster

Agregación de una réplica a un clúster de Amazon DocumentDB

Después de crear la instancia principal de su clúster de Amazon DocumentDB, puede añadir una o varias réplicas. Una réplica es una instancia de solo lectura que tiene dos finalidades:

- Escalabilidad: si tiene gran cantidad de clientes que deben obtener acceso simultáneamente, puede agregar más réplicas para escalar la lectura.
- Alta disponibilidad: si se produce un error en la instancia primaria, Amazon DocumentDB automáticamente realiza una conmutación por error a una instancia de réplica y la designa como nuevo nodo primario. Si se produce un error en una réplica, otras instancias del clúster pueden seguir atendiendo las solicitudes hasta que se consigue recuperar el nodo defectuoso.

Cada clúster de Amazon DocumentDB puede admitir hasta 15 réplicas.

> **Note**
>
> Para disfrutar de la máxima tolerancia a errores, debe implementar réplicas en zonas de disponibilidad distintas. Esta configuración garantiza que el clúster de Amazon DocumentDB continúe funcionando aunque una zona de disponibilidad completa deje de estar disponible.

En el ejemplo siguiente de la AWS CLI, se muestra cómo añadir una nueva réplica. El parámetro `--availability-zone` coloca la réplica en la zona de disponibilidad especificada

```
aws docdb create-db-instance \
    --db-instance-identifier sample-instance \
    --db-cluster-identifier sample-cluster \
    --engine docdb \
    --db-instance-class db.r5.large \
    --availability-zone us-east-1a
```

Descripción de clústeres e instancias

En el siguiente ejemplo de la AWS CLI se enumeran todos los clústeres de Amazon DocumentDB de una región. Para ciertas características de administración, como la administración del ciclo de vida de clúster y de instancia, Amazon DocumentDB aprovecha la tecnología operativa que se comparte con Amazon RDS. El parámetro de filtro `filterName=engine,Values=docdb` devuelve solo clústeres de Amazon DocumentDB.

Para obtener más información sobre cómo describir y modificar clústeres, consulte Ciclo de vida del clúster de Amazon DocumentDB.

```
aws docdb describe-db-clusters --filter Name=engine,Values=docdb
```

La salida de esta operación será similar a lo que se indica a continuación.

```
{
    "DBClusters": [
        {
            "AvailabilityZones": [
                "us-east-1c",
                "us-east-1b",
                "us-east-1a"
            ],
            "BackupRetentionPeriod": 1,
            "DBClusterIdentifier": "sample-cluster-1",
            "DBClusterParameterGroup": "sample-parameter-group",
            "DBSubnetGroup": "default",
            "Status": "available",
            ...
        },
```

```
        {
            "AvailabilityZones": [
                "us-east-1c",
                "us-east-1b",
                "us-east-1a"
            ],
            "BackupRetentionPeriod": 1,
            "DBClusterIdentifier": "sample-cluster-2",
            "DBClusterParameterGroup": "sample-parameter-group",
            "DBSubnetGroup": "default",
            "Status": "available",
            ...
        },
        {
            "AvailabilityZones": [
                "us-east-1c",
                "us-east-1b",
                "us-east-1a"
            ],
            "BackupRetentionPeriod": 1,
            "DBClusterIdentifier": "sample-cluster-3",
            "DBClusterParameterGroup": "sample-parameter-group",
            "DBSubnetGroup": "default",
            "Status": "available",
            ...
        }
    ]
}
```

En el siguiente ejemplo de la AWS CLI se muestran las instancias de un clúster de Amazon DocumentDB. Para obtener más información sobre cómo describir y modificar clústeres, consulte Ciclo de vida de instancia de Amazon DocumentDB.

```
aws docdb describe-db-clusters \
    --db-cluster-identifier sample-cluster \
    --query 'DBClusters[*].[DBClusterMembers]'
```

El resultado es similar al siguiente. En este resultado hay dos instancias. La instancia principal es `sample-instance-1` (`"IsClusterWriter": true`). También hay una instancia de réplica, `sample-instance2` (`"IsClusterWriter: false"`).

```
[
```

```
    [
        [
            {
                "DBInstanceIdentifier": "sample-instance-1",
                "IsClusterWriter": true,
                "DBClusterParameterGroupStatus": "in-sync",
                "PromotionTier": 1
            },
            {
                "DBInstanceIdentifier": "sample-cluster-2",
                "IsClusterWriter": false,
                "DBClusterParameterGroupStatus": "in-sync",
                "PromotionTier": 1
            }
        ]
    ]
]
```

Creación de una instantánea de un clúster

Una instantánea de clúster es una copia de seguridad completa de los datos del clúster de Amazon DocumentDB. Cuando la instantánea se está creando, Amazon DocumentDB lee los datos directamente del volumen del clúster. Por este motivo, puede crear una instantánea aunque el clúster no tenga instancias en ejecución en ese momento. La cantidad de tiempo que tarda en crearse una instantánea depende del tamaño del volumen del clúster.

Amazon DocumentDB admite copias de seguridad automáticas, que se realizan a diario durante el período de copia de seguridad preferido, es decir, un período de 30 minutos durante el día. En el siguiente ejemplo de la AWS CLI se muestra cómo ver el periodo de copia de seguridad del clúster:

```
aws docdb describe-db-clusters \
    --db-cluster-identifier sample-cluster \
    --query 'DBClusters[*].PreferredBackupWindow'
```

El resultado muestra el periodo de copia de seguridad (en UTC):

```
[
    "00:18-00:48"
]
```

Puede definir el periodo de copia de seguridad cuando cree el clúster de Amazon DocumentDB. También puede cambiar el periodo de copia de seguridad, tal y como se muestra en el siguiente ejemplo: Si no define un periodo de copia de seguridad, Amazon DocumentDB asigna uno automáticamente a su clúster.

```
aws docdb modify-db-cluster \
    --db-cluster-identifier sample-cluster \
    --preferred-backup-window "02:00-02:30"
```

Además de copias de seguridad automáticas, puede crear manualmente una instantánea del clúster en cualquier momento. Cuando cree la instantánea, especifique el clúster del que desea hacer una copia de seguridad y un nombre único para la instantánea, de forma que pueda realizar la restauración desde ella en otro momento.

El ejemplo de la AWS CLI siguiente muestra cómo crear una instantánea de los datos.

```
aws docdb create-db-cluster-snapshot \
    --db-cluster-identifier sample-cluster \
    --db-cluster-snapshot-identifier sample-cluster-snapshot
```

Restauración a partir de una instantánea

Puede restaurar una instantánea de clúster en un nuevo clúster de Amazon DocumentDB. Para ello, proporcione el nombre de la instantánea y el nombre de un nuevo clúster. No puede restaurar desde una instantánea a un clúster existente; en su lugar, Amazon DocumentDB crea un nuevo clúster al restaurar y, a continuación, lo rellena con los datos de su instantánea.

El siguiente ejemplo muestra todas las instantáneas de un clúster `sample-cluster`.

```
aws docdb describe-db-cluster-snapshots \
    --db-cluster-identifier sample-cluster \
    --query 'DBClusterSnapshots[*].[DBClusterSnapshotIdentifier,SnapshotType,Status]'
```

El resultado es similar al siguiente. Una instantánea manual es aquella que se crea manualmente, mientras que una instantánea automatizada la crea Amazon DocumentDB dentro del periodo de copia de seguridad del clúster.

```
[
```

```
        "sample-cluster-snapshot",
        "manual",
        "available"
    ],
    [
        "rds:sample-cluster",
        "automated",
        "available"
    ]
]
```

En el siguiente ejemplo se muestra cómo restaurar un clúster de Amazon DocumentDB a partir de una instantánea.

```
aws docdb restore-db-cluster-from-snapshot \
    --engine docdb \
    --db-cluster-identifier new-sample-cluster \
    --snapshot-identifier sample-cluster-snapshot
```

El nuevo clúster no tiene instancias asociadas; por lo tanto, si desea interactuar con el clúster, debe añadirle una instancia.

```
aws docdb create-db-instance \
    --db-instance-identifier new-sample-instance \
    --db-instance-class db.r5.large \
    --engine docdb \
    --db-cluster-identifier new-sample-cluster
```

Puede utilizar las siguientes operaciones de la AWS CLI para monitorizar el progreso de creación del clúster y de la instancia. Cuando el clúster y la instancia tengan estados disponibles, podrá conectarse al punto de conexión del nuevo clúster y obtener acceso a sus datos.

```
aws docdb describe-db-clusters \
    --db-cluster-identifier new-sample-cluster  \
    --query 'DBClusters[*].[Status,Endpoint]'
```

```
aws docdb describe-db-instances \
    --db-instance-identifier new-sample-instance \
    --query 'DBInstances[*].[DBInstanceStatus]'
```

Eliminación de una instancia de un clúster

Amazon DocumentDB almacena todos los datos en el volumen del clúster. Los datos se conservan en ese volumen de clúster, incluso si elimina todas las instancias del clúster. Si necesita obtener acceso a los datos de nuevo, puede añadir una instancia a la clúster en cualquier momento y reanudar el trabajo donde lo dejó.

En el siguiente ejemplo se muestra cómo eliminar una instancia de su clúster de Amazon DocumentDB.

```
aws docdb delete-db-instance \
    --db-instance-identifier sample-instance
```

Eliminación de un clúster

Para poder eliminar un clúster de Amazon DocumentDB, primero debe eliminar todas sus instancias. En el siguiente ejemplo de la AWS CLI, se devuelve información acerca de las instancias de un clúster. Si esta operación devuelve algún identificador de instancia, tendrá que eliminar cada una de esas instancias. Para obtener más información, consulte Eliminación de una instancia de un clúster.

```
aws docdb describe-db-clusters \
    --db-cluster-identifier sample-cluster \
    --query 'DBClusters[*].DBClusterMembers[*].DBInstanceIdentifier'
```

Cuando no queden más instancias, puede eliminar el clúster. En ese momento, debe elegir una de las siguientes opciones:

- Cree una instantánea final: capture todos los datos del clúster en una instantánea para poder volver a crear una nueva instancia con esos datos más adelante. El siguiente ejemplo le muestra cómo hacerlo:

  ```
  aws docdb delete-db-cluster \
      --db-cluster-identifier sample-cluster \
      --final-db-snapshot-identifier sample-cluster-snapshot
  ```

- Omita la instantánea final: descarte permanentemente todos los datos del clúster. Esta operación no se puede deshacer. El siguiente ejemplo le muestra cómo hacerlo:

  ```
  aws docdb delete-db-cluster \
      --db-cluster-identifier sample-cluster \
  ```

```
    --skip-final-snapshot
```

Información general de los clústeres globales de Amazon DocumentDB

¿Qué es un clúster global?

Un clúster global consta de una región principal y hasta 10 regiones secundarias de solo lectura. Usted emite operaciones de escritura directamente en el clúster primario de la región primaria y Amazon DocumentDB replica automáticamente los datos en las regiones secundarias utilizando una infraestructura dedicada. La latencia suele ser inferior a un segundo.

¿Para qué sirven los clústeres globales?

- Recuperación de interrupciones en toda la región: si se produce una interrupción en toda la región, puede convertir uno de los clústeres secundarios en un clúster primario en cuestión de minutos, con un objetivo de tiempo de recuperación (RTO) típico de menos de un minuto. El objetivo de punto de recuperación (RPO) suele medirse en segundos, pero depende del desfase existente en la red en el momento del fallo.
- Lecturas globales con latencia local - Si tiene oficinas en todo el mundo, puede utilizar un clúster global para mantener actualizadas sus principales fuentes de información en la región principal. Las oficinas en sus otras regiones pueden acceder a la información en su propia región, con latencia local.
- Clústeres secundarios escalables - Puede escalar los clústeres secundarios agregando más instancias de solo lectura a una región secundaria. El clúster secundario es de solo lectura, por lo que puede admitir hasta 16 instancias de réplica de solo lectura en lugar del límite habitual de 15 para un solo clúster.
- Replicación rápida de clústeres primarios a secundarios - La replicación realizada por un clúster global tiene poco impacto en el performance en el clúster primario. Los recursos de las instancias de bases de datos están totalmente dedicados a servir a las cargas de trabajo de lectura y escritura de la aplicación.

¿Cuáles son las limitaciones actuales de los clústeres globales?

- Los clústeres globales no son compatibles con Amazon DocumentDB v3.6.

- Los clústeres globales no son compatibles con los tipos de instancia t3, t4g y r4.
- Los clústeres globales no están disponibles en las siguientes regiones: América del Sur (São Paulo), Europa (Milán), China (Pekín) y China (Ningxia).
- La transición y la conmutación por error global no se admiten cuando las regiones tienen versiones de motor diferentes. Se admite la conmutación por error manual cuando existe una discordancia entre las versiones del motor.
- Solo el clúster primario realiza operaciones de escritura. Los clientes que realizan operaciones de escritura se conectan al punto de conexión del clúster primario.
- Puede tener un máximo de 10 regiones secundarias y una región principal para su clúster.
- No se puede detener un clúster secundario. No se puede detener un clúster primario si tiene clústeres secundarios asociados. Solo se puede detener un clúster regional que no tenga clústeres secundarios.
- Las réplicas conectadas al clúster secundario pueden reiniciarse en determinadas circunstancias. Si la instancia de la región primaria se reinicia o falla, las réplicas de la región secundaria también se reinician. El clúster no estará disponible hasta que todas las réplicas estén nuevamente sincronizadas con la instancia del escritor del clúster de base de datos principal. Este es el comportamiento esperado. Asegúrese de comprender los impactos en la base de datos global antes de realizar cambios en el clúster primario.
- No se pueden utilizar flujos de cambios en clústeres secundarios.

Temas

- Guía de inicio rápido: clústeres globales
- Administración de un clúster global de Amazon DocumentDB
- Conexión a un clúster global de Amazon DocumentDB
- Supervisión de clústeres globales de Amazon DocumentDB
- Recuperación ante desastres y clústeres globales de Amazon DocumentDB

Guía de inicio rápido: clústeres globales

Temas

- Configuración
- Creación de un clúster global de Amazon DocumentDB
- Cómo agregar una Región de AWS a un clúster global de Amazon DocumentDB

- Uso de una instantánea para el clúster global de Amazon DocumentDB

Configuración

El clúster global de Amazon DocumentDB abarca al menos dos Regiones de AWS. La región principal admite un clúster que tiene una instancia principal (de escritura) y hasta 15 instancias de réplica, mientras que la región secundaria ejecuta un clúster de solo lectura compuesto en su totalidad por un máximo de 16 instancias de réplica. Un clúster global puede tener hasta cinco regiones secundarias. La tabla muestra el máximo de clústeres, instancias y réplicas permitidos en clúster global.

Descripción	principal Región de AWS	secundaria Región de AWS
Clústeres	1	5 (máximo)
Instancias de escritor	1	0
Instancias de solo lectura (réplicas de Amazon DocumentDB), por clúster	15 (máx.)	16 (total)
Instancias de solo lectura (máximo permitido, dado el número real de Regiones secundarias)	15 - s	s = total de Regiones de AWS secundarias

Los clústeres tienen los siguientes requisitos específicos:

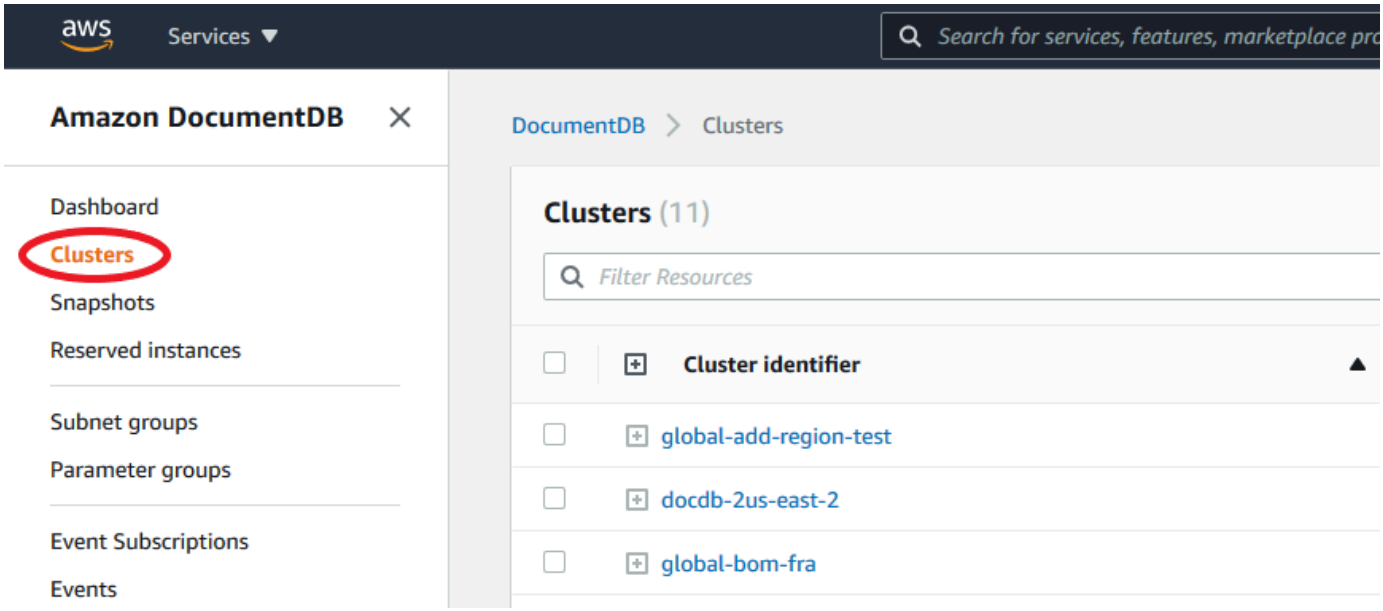
- Requisitos de clase de instancia de base de datos: solo puede usar las clases de instancia `db.r5` y `db.r6g`.
- Requisitos de la Región de AWS: el clúster principal debe estar en una región y, al menos, un clúster secundario debe estar en una región diferente de la misma cuenta. Puede crear hasta cinco clústeres secundarios (de solo lectura) y cada uno debe estar en una región diferente. En otras palabras, no puede haber dos clústeres en la misma región.
- Requisitos de nomenclatura: los nombres que elija para cada uno de los clústeres deben ser únicos, en todas las regiones. No puede usar el mismo nombre para diferentes clústeres aunque estén en diferentes regiones.

Creación de un clúster global de Amazon DocumentDB

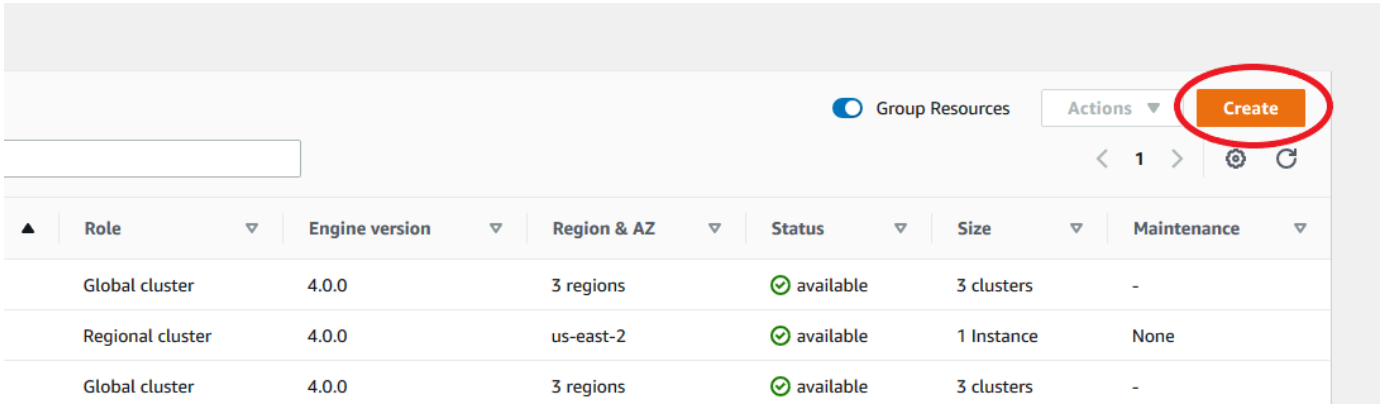
¿Está preparado para compilar su primer clúster global? En esta sección, explicaremos cómo crear un clúster global completamente nuevo con nuevos clústeres e instancias de bases de datos, utilizando la Consola de administración de AWS o la AWS CLI siguiendo estas instrucciones.

Uso de Consola de administración de AWS

1. En la Consola de administración de AWS, vaya a Amazon DocumentDB.
2. Cuando llegue a la consola de Amazon DocumentDB, elija Clústeres.

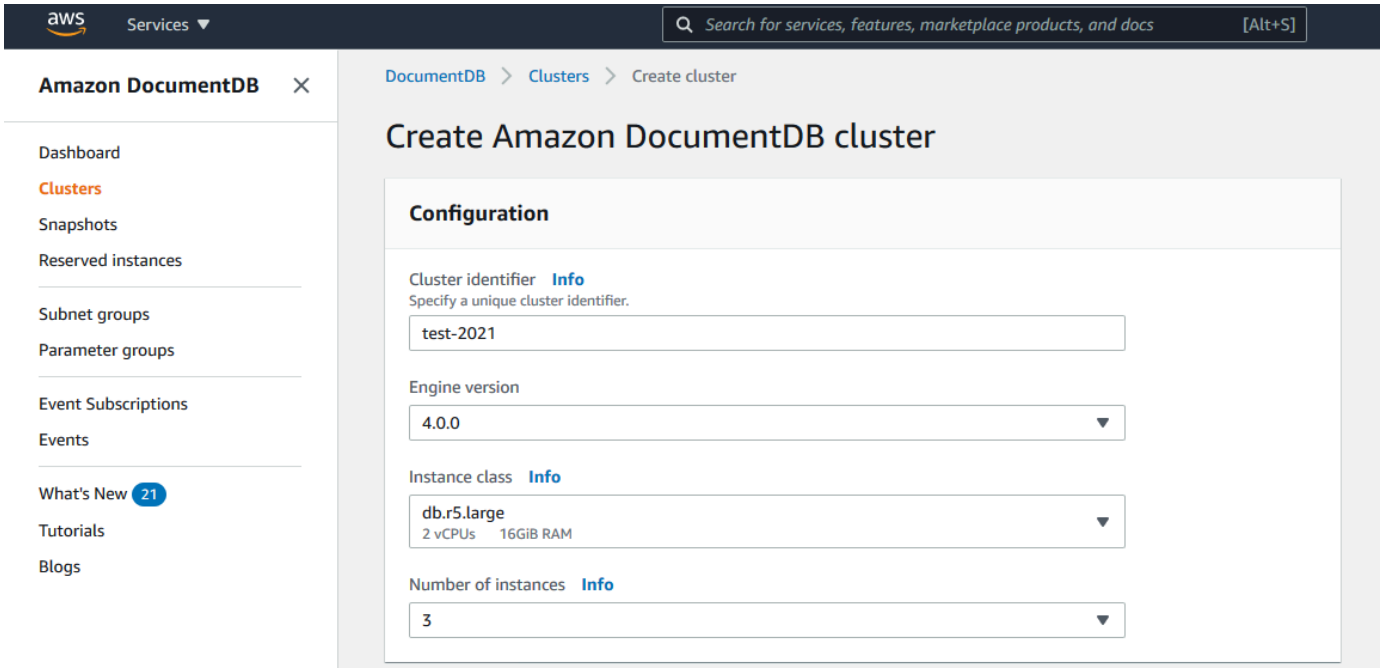


3. Seleccione Crear.

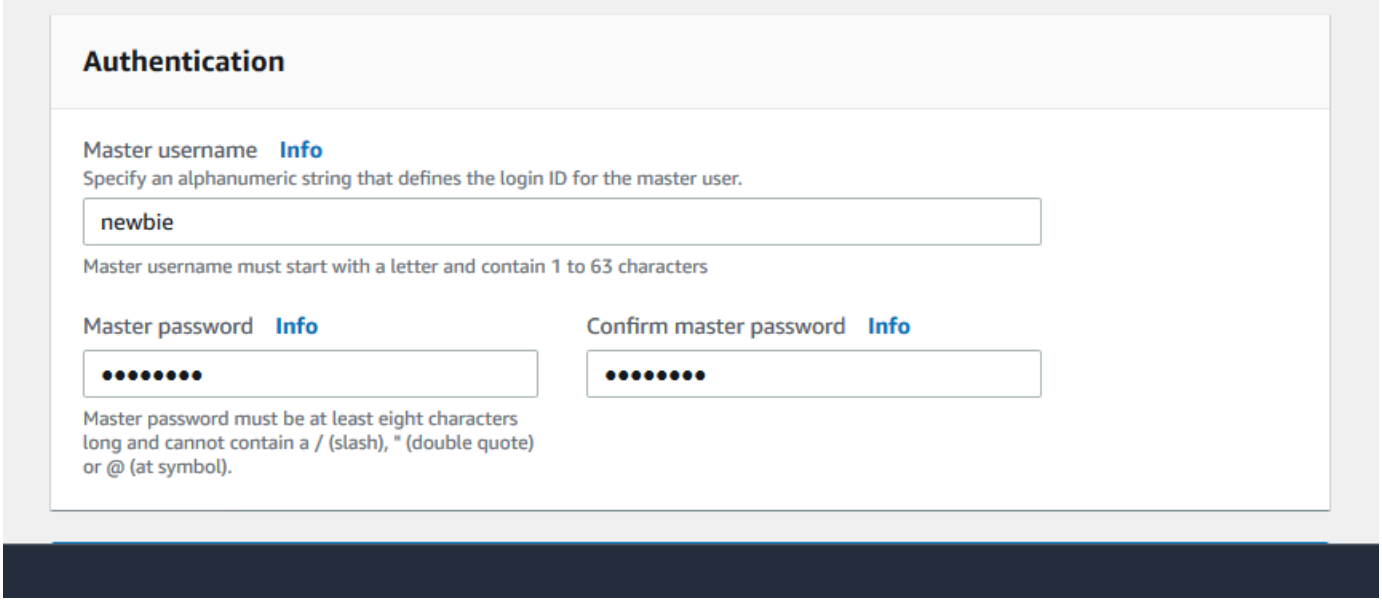


4. Rellene la sección Configuración del formulario Crear un clúster de Amazon DocumentDB según corresponda:

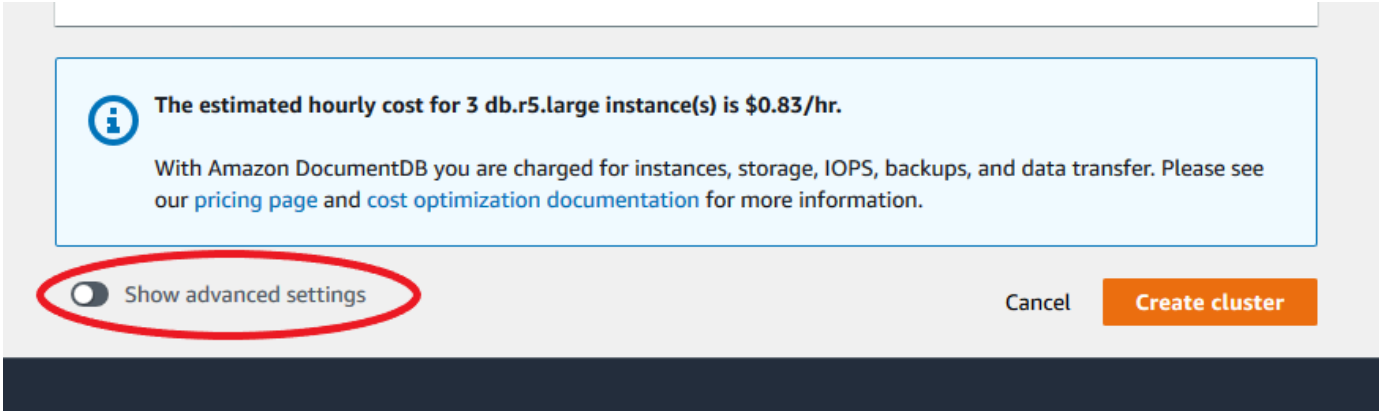
- Identificador de clúster puede escribir un identificador único para esta instancia o permitir que Amazon DocumentDB proporcione el identificador de la instancia basándose en el identificador del clúster.
- Elija la versión del motor 4.0.0
- Clase de instancia: elija db.r5.large
- Número de instancias: elija 3.



5. En la sección Autenticación, introduzca un nombre de usuario maestro y una contraseña maestra.

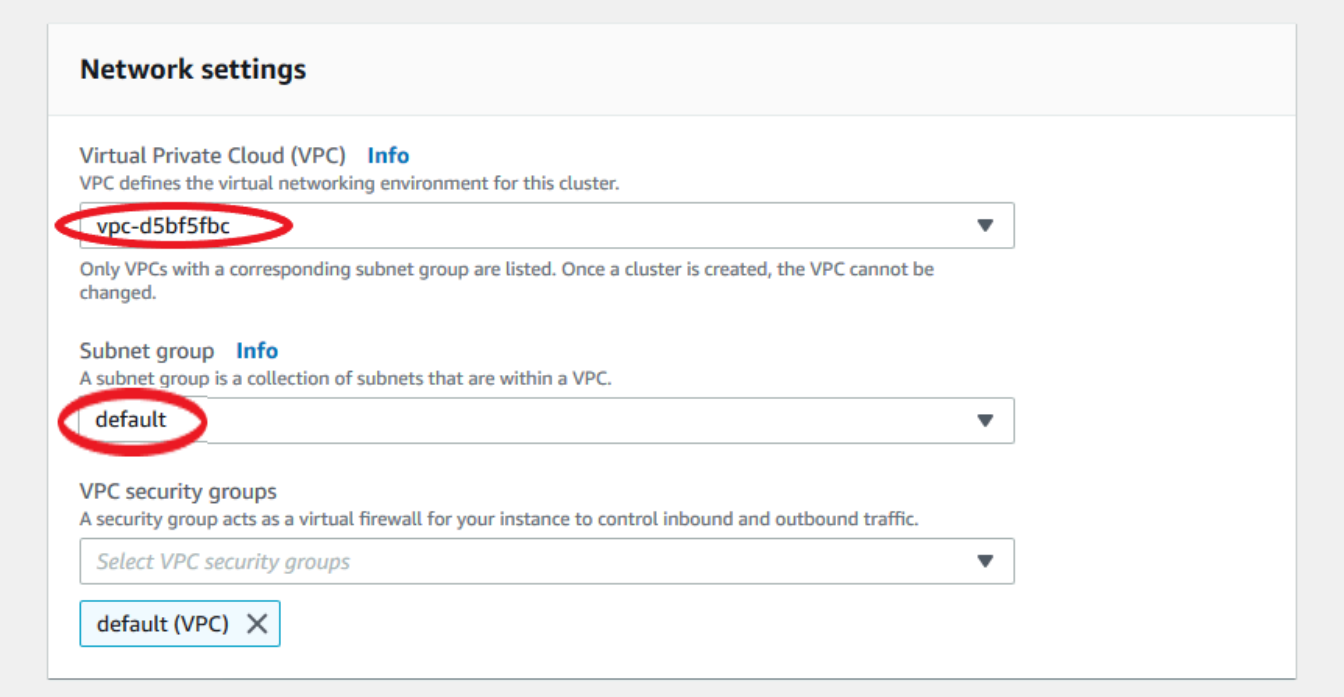


6. Seleccione Mostrar configuración avanzada.

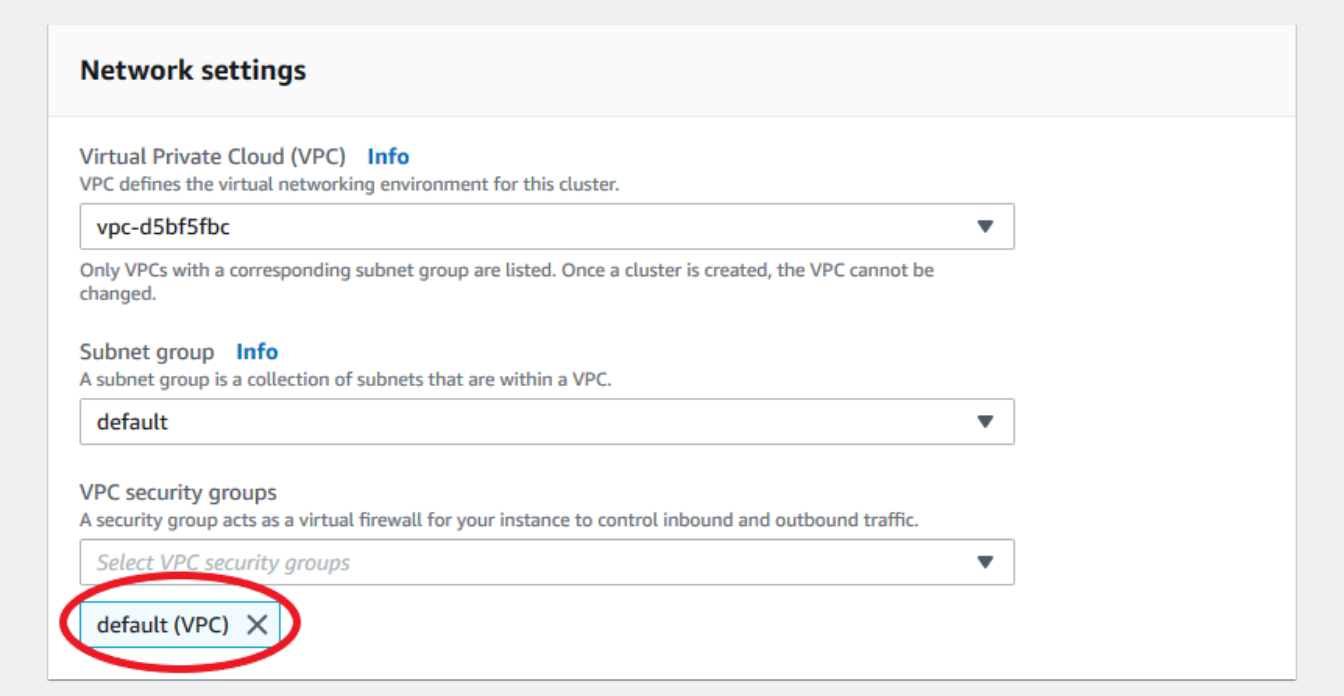


7. En la sección Configuración de red:

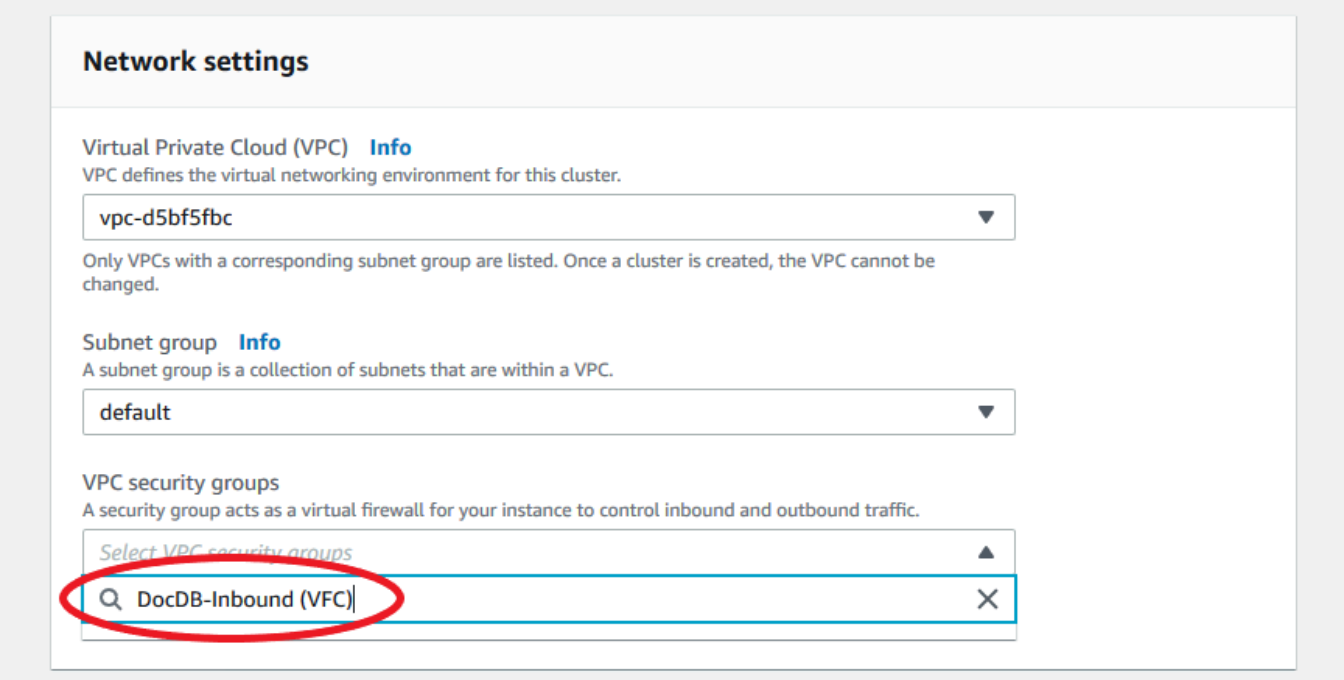
   - Mantenga las opciones predeterminadas para la Nube privada virtual (VPC) y el Grupo de subredes.



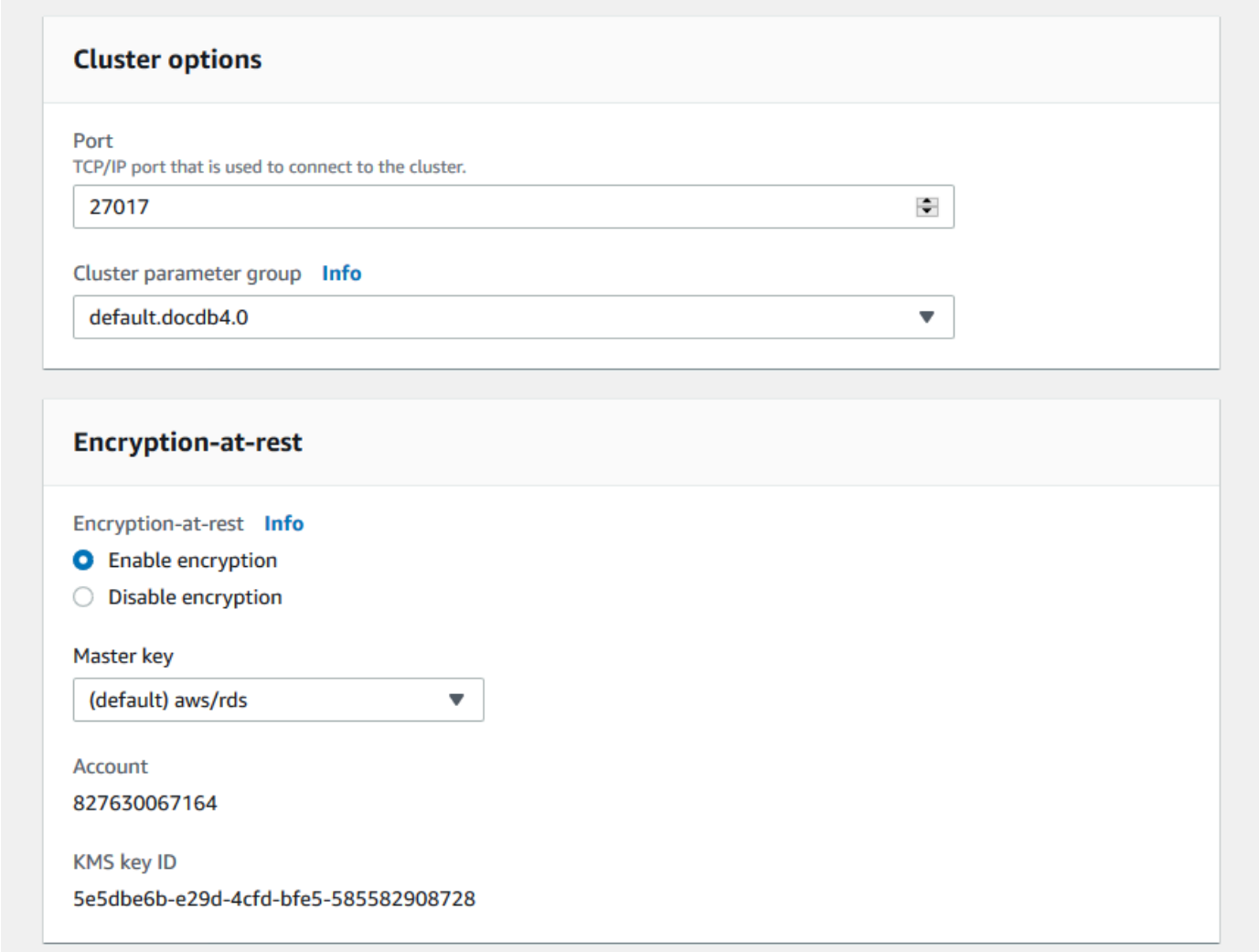
- Para los grupos de seguridad de VPC, la (VPC) predeterminada ya debería estar añadida.



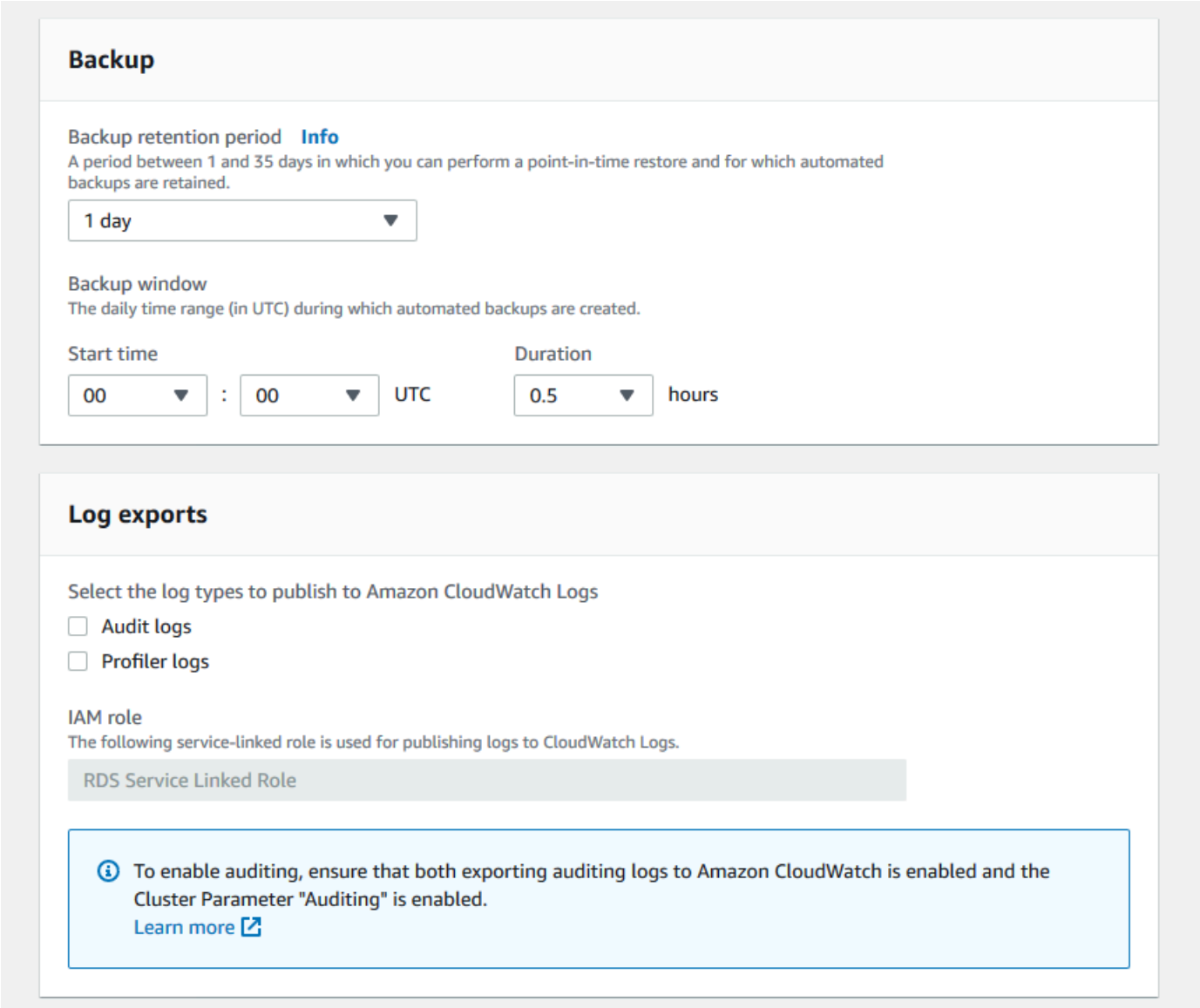
- Escriba `DocDB` en el campo Grupos de seguridad de VPC y seleccione DocDB-Inbound (VFC).



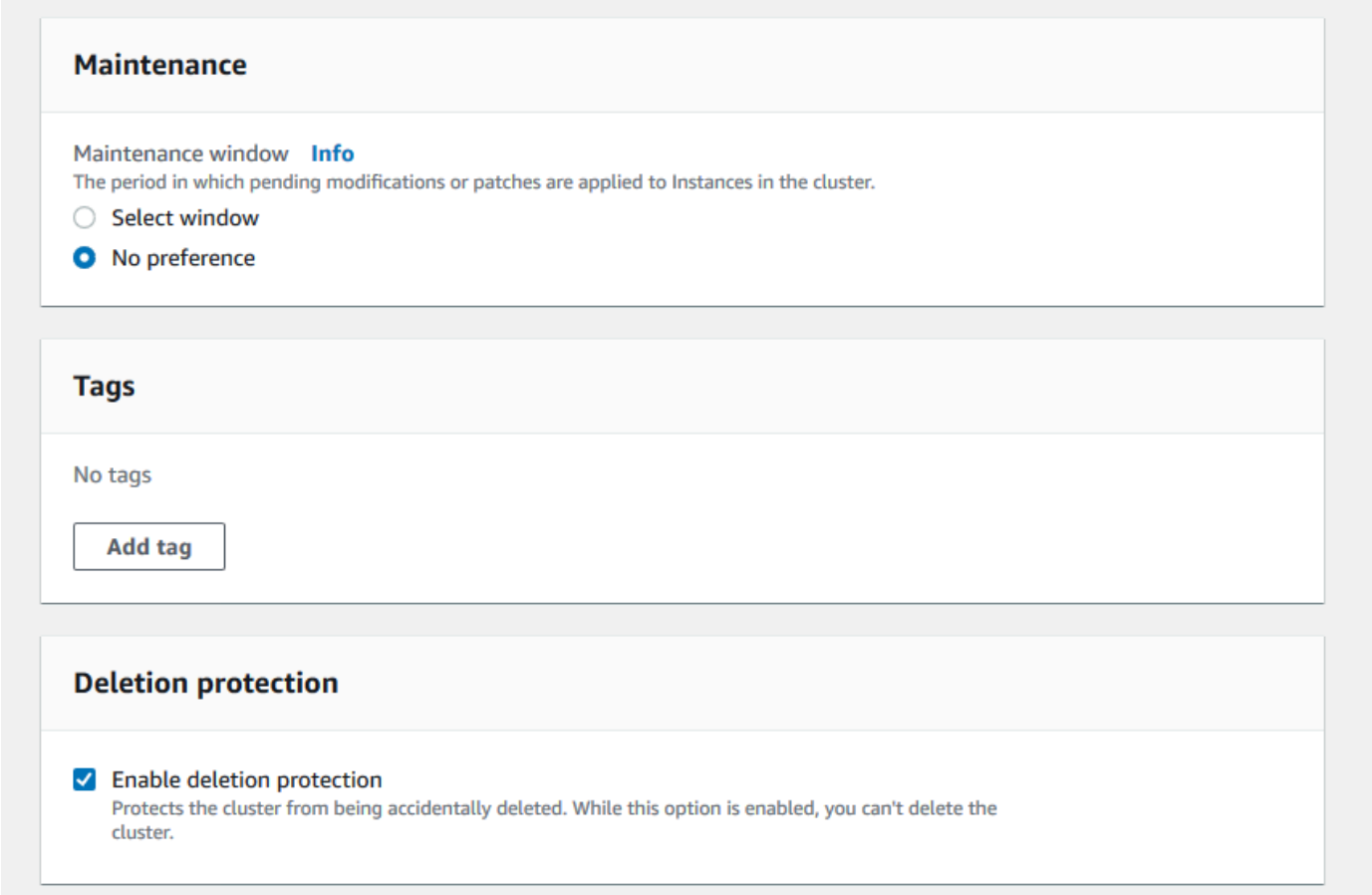
8. En Opciones de clúster y Cifrado en reposo, deje las selecciones predeterminadas.



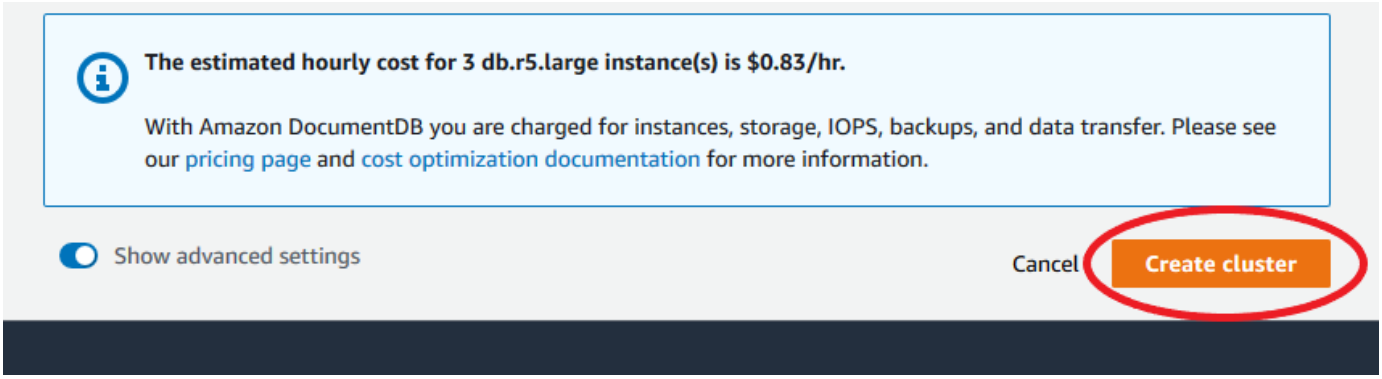
9. Para Copia de seguridad y Exportaciones de registros, deje las selecciones predeterminadas.



10. Para Mantenimiento, Etiquetas y Protección contra eliminación, deje las selecciones predeterminadas.



11. Ahora haga clic en el botón que dice Crear clúster.



Uso de AWS CLI

Para crear un clúster regional de Amazon DocumentDB, llame a la AWS CLI create-global-cluster. El siguiente comando de la AWS CLI crea un clúster de Amazon DocumentDB denominado `global-cluster-id`. Para obtener más información sobre la protección contra eliminación, consulte Eliminación de un clúster de Amazon DocumentDB.

Además, `--engine-version` es un parámetro opcional que utiliza de forma predeterminada la última versión principal del motor. La versión principal del motor es `5.0.0`. Cuando se publiquen nuevas versiones principales del motor, la versión del motor predeterminada para `--engine-version` se actualizará para reflejar la última versión principal del motor. Por lo tanto, para las cargas de trabajo de producción, y especialmente las que dependen de la creación de scripts, la automatización o las plantillas CloudFormation, le recomendamos que especifique explícitamente la `--engine-version` en la versión principal prevista.

Si no se especifica un `db-subnet-group-name` o un `vpc-security-group-id`, Amazon DocumentDB utilizará el grupo de subredes y el grupo de seguridad de Amazon VPC predeterminados para la región determinada.

En el siguiente ejemplo, reemplace cada *`marcador de posición del usuario`* con su propia información.

Para Linux, macOS o Unix:

```
aws docdb create-db-cluster \
      --global-cluster-identifier global-cluster-id \
      --source-db-cluster-identifier arn:aws:rds:us-east-1:111122223333:cluster-id
```

Para Windows:

```
aws docdb create-db-cluster ^
      --global-cluster-identifier global-cluster-id ^
      --source-db-cluster-identifier arn:aws:rds:us-east-1:111122223333:cluster-id
```

La salida de esta operación será similar a lo que se indica a continuación (formato JSON).

```
{
    "DBCluster": {
        "StorageEncrypted": false,
        "DBClusterMembers": [],
        "Engine": "docdb",
        "DeletionProtection" : "enabled",
        "ClusterCreateTime": "2018-11-26T17:15:19.885Z",
        "DBSubnetGroup": "default",
        "EngineVersion": "4.0.0",
```

```
        "MasterUsername": "masteruser",
        "BackupRetentionPeriod": 1,
        "DBClusterArn": "arn:aws:rds:us-east-1:123456789012:cluster:cluster-id",
        "DBClusterIdentifier": "cluster-id",
        "MultiAZ": false,
        "DBClusterParameterGroup": "default.docdb4.0",
        "PreferredBackupWindow": "09:12-09:42",
        "DbClusterResourceId": "cluster-KQSGI4MHU4NTDDRVNLNTU7XVAY",
        "PreferredMaintenanceWindow": "tue:04:17-tue:04:47",
        "Port": 27017,
        "Status": "creating",
        "ReaderEndpoint": "cluster-id.cluster-ro-sfcrlcjcoroz.us-
east-1.docdb.amazonaws.com",
        "AssociatedRoles": [],
        "HostedZoneId": "ZNKXTT8WH85VW",
        "VpcSecurityGroups": [
            {
                "VpcSecurityGroupId": "sg-77186e0d",
                "Status": "active"
            }
        ],
        "AvailabilityZones": [
            "us-east-1a",
            "us-east-1c",
            "us-east-1e"
        ],
        "Endpoint": "cluster-id.cluster-sfcrlcjcoroz.us-east-1.docdb.amazonaws.com"
    }
}
```

La creación del clúster puede tardar varios minutos. Puede utilizar la Consola de administración de AWS o la AWS CLI para monitorizar el estado de su clúster. Para obtener más información, consulte Supervisión del estado de un clúster de Amazon DocumentDB.

> **Important**
>
> Cuando se utiliza la AWS CLI para crear un clúster regional de Amazon DocumentDB, no se crea ninguna instancia. Por lo tanto, tendrá que crear de forma explícita una instancia principal y las instancias de réplica que necesite. Puede utilizar la consola o la AWS CLI para crear las instancias. Para obtener más información, consulte Agregación de una instancia de

Amazon DocumentDB a un clúster y CreateDBCluster en la Referencia de la API de Amazon DocumentDB.

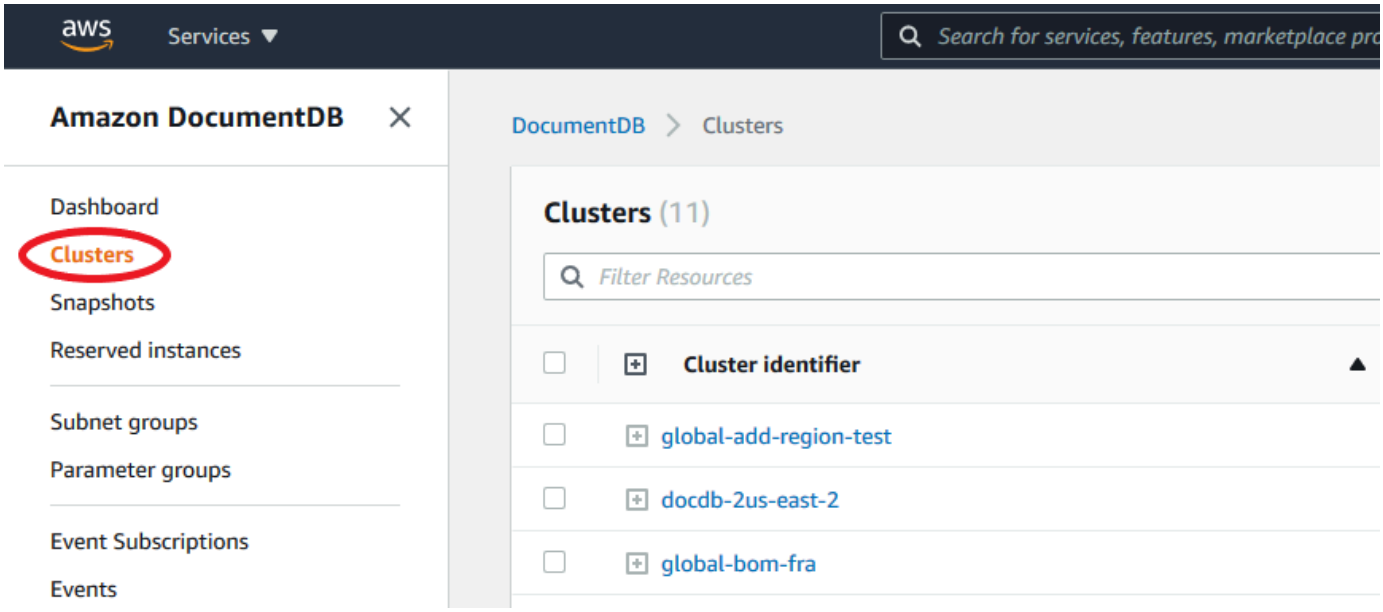
Una vez que su clúster regional esté disponible, puede añadir un clúster secundario en otra región con las siguientes instrucciones: Cómo agregar una Región de AWS a un clúster global de Amazon DocumentDB. Cuando añada una región, su clúster regional se convierte en su clúster principal y tiene un nuevo clúster secundario en la región que ha elegido.

Cómo agregar una Región de AWS a un clúster global de Amazon DocumentDB

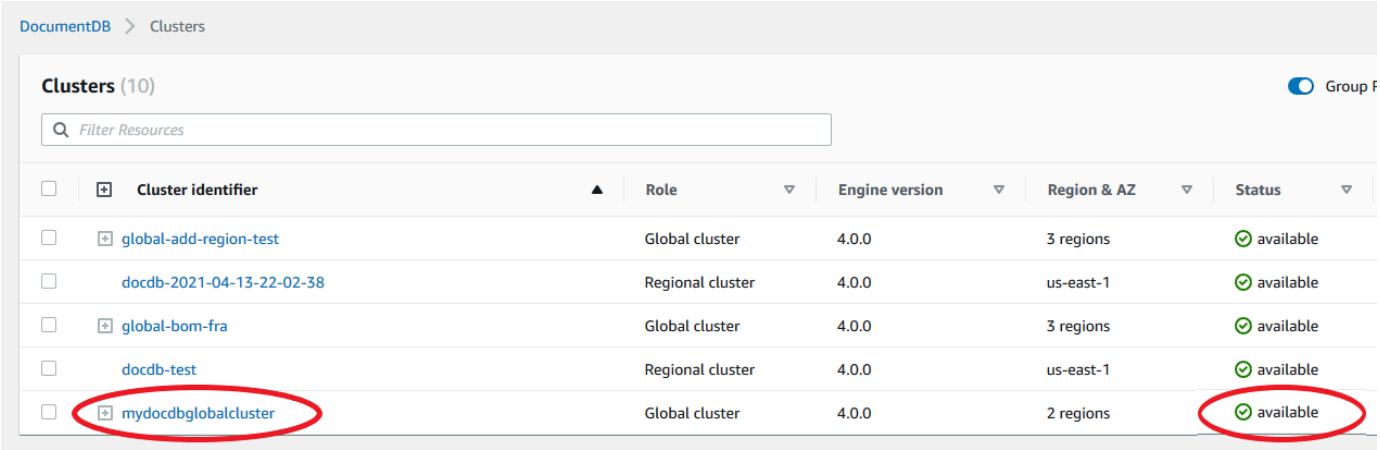
Un clúster global necesita al menos un clúster secundario en una región diferente a la del clúster principal, y puede añadir hasta cinco clústeres secundarios. Para cada clúster secundario que agregue, deberá reducir el número de réplicas permitidas al clúster principal en una. Por ejemplo, si su clúster global tiene cinco regiones secundarias, el clúster principal puede tener solamente 10 (en lugar de 15) réplicas. Para obtener más información, consulte Requisitos de configuración de un clúster global de Amazon DocumentDB.

Uso de Consola de administración de AWS

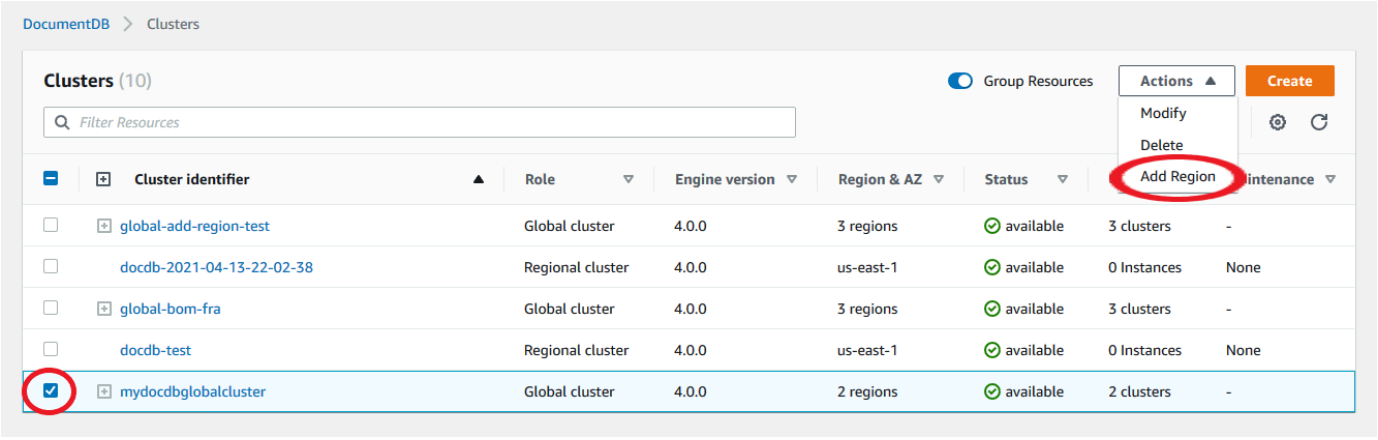
1. Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon DocumentDB.
2. En el panel de navegación, seleccione Clusters (Clústeres).



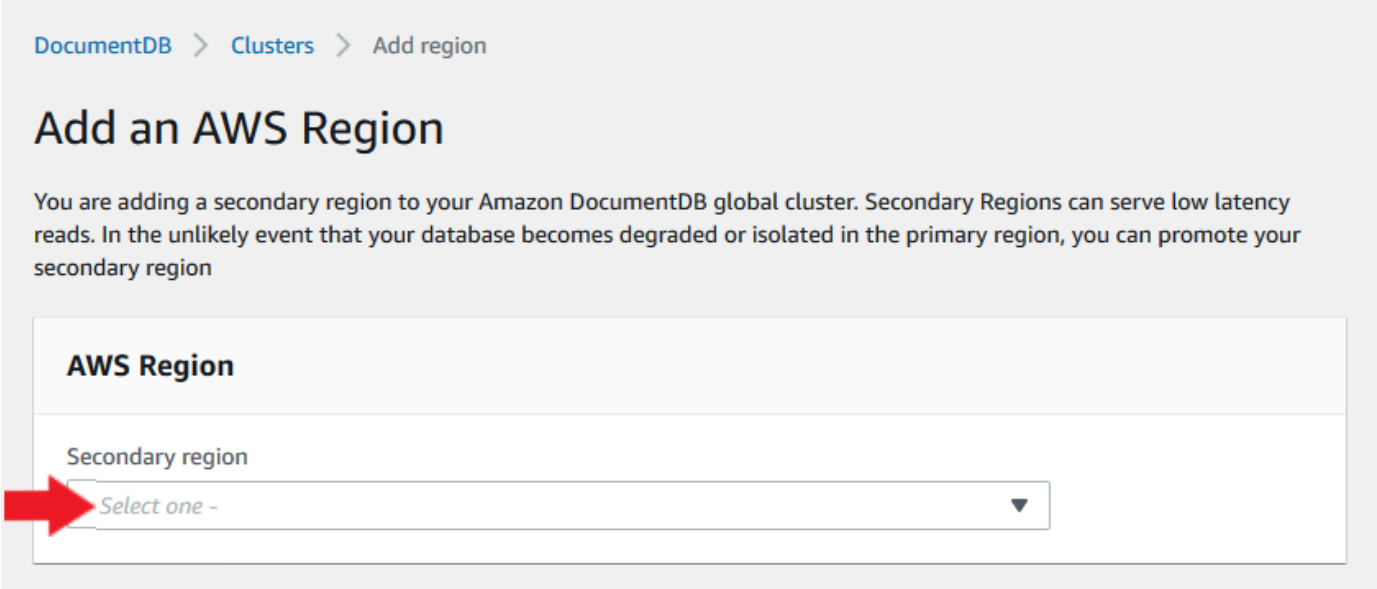
3. Elija el clúster al que desearía agregar un clúster secundario. Asegúrese de que el clúster es `Available`.



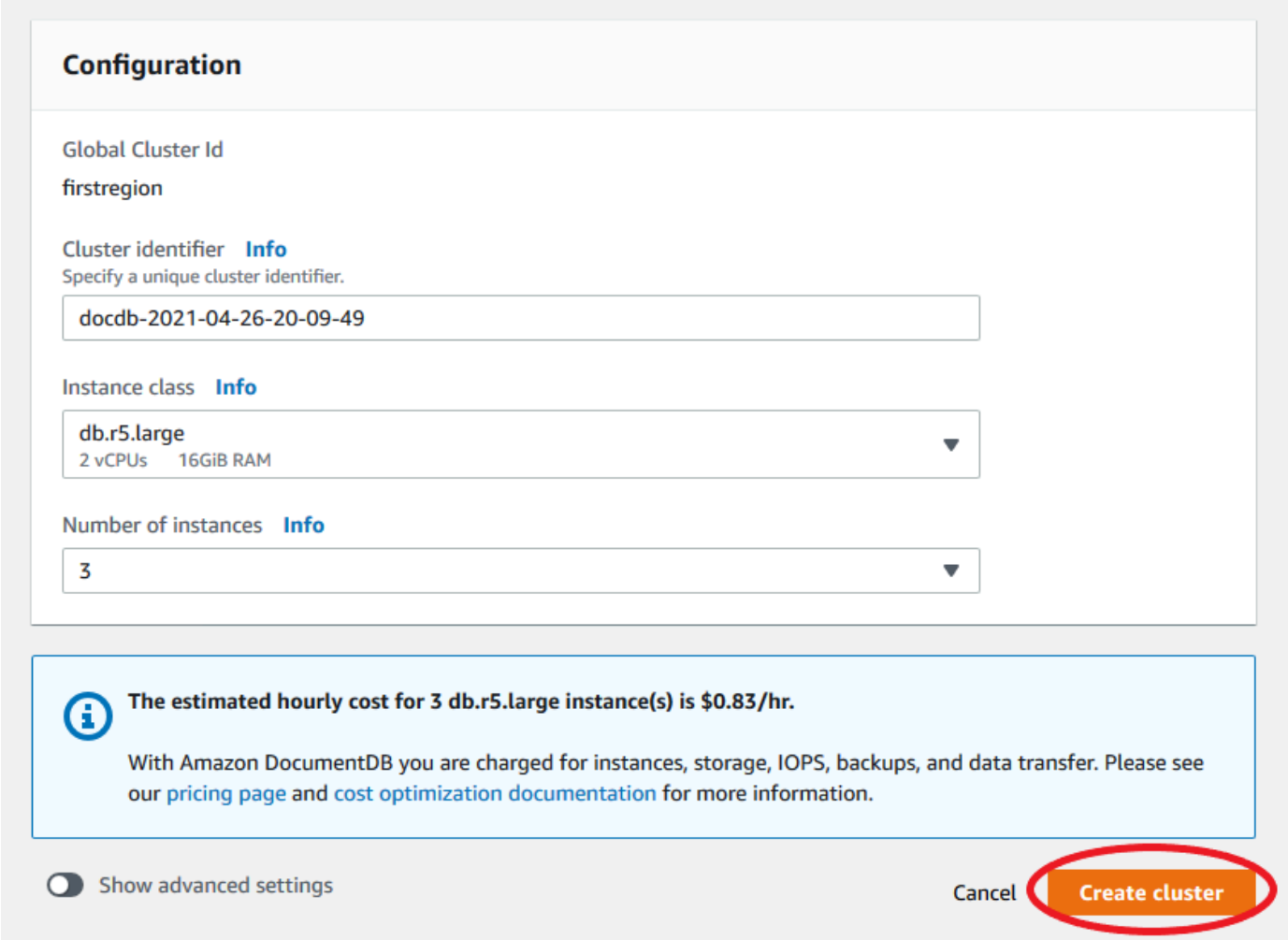
4. Seleccione el menú desplegable Acciones y, a continuación, seleccione Añadir región.



5. En la página Añadir una Región de AWS, seleccione la región secundaria. No puede elegir una región que ya tenga un clúster secundario para el mismo clúster global. Además, no puede ser la misma región que el clúster principal. Si es la primera región que va a añadir, también tendrá que especificar un identificador de clúster global de su elección.



6. Complete los campos restantes para el clúster secundario en la nueva región, luego seleccione Crear clúster. Después de terminar de añadir la región, puede verla en la lista de Clústeres en la Consola de administración de AWS.



Uso de AWS CLI

- Utilice el comando `create-db-cluster` CLI con el nombre (`--global-cluster-identifier`) del clúster global. Para otros parámetros, haga lo siguiente:
  - Para `--region`, elija una Región de AWS diferente a la de su región principal.
  - Elija valores específicos para los parámetros `--engine` y `--engine-version`.
  - Para un clúster cifrado, especifique la Región de AWS principal como `--source-region` para cifrado.

En el ejemplo siguiente se crea un nuevo clúster de Amazon DocumentDB y se adjunta al clúster global como clúster secundario de solo lectura. En el último paso, se agrega una instancia al nuevo clúster.

En el siguiente ejemplo, reemplace cada *marcador de posición del usuario* con su propia información.

Para Linux, macOS o Unix:

```
aws docdb --region secondary-region-id \
  create-db-cluster \
    --db-cluster-identifier cluster-id \
    --global-cluster-identifier global-cluster-id \
    --engine-version version \
    --engine docdb

aws docdb --region secondary-region-id \
  create-db-instance \
    --db-cluster-identifier cluster-id \
    --global-cluster-identifier global-cluster-id \
    --engine-version version \
    --engine docdb
```

Para Windows:

```
aws docdb --region secondary-region-id ^
  create-db-cluster ^
    --db-cluster-identifier cluster-id ^
    --global-cluster-identifier global-cluster-id ^
    --engine-version version ^
    --engine docdb

aws docdb --region secondary-region-id ^
  create-db-instance ^
    --db-cluster-identifier cluster-id ^
    --global-cluster-identifier global-cluster-id ^
    --engine-version version ^
    --engine docdb
```

Uso de una instantánea para el clúster global de Amazon DocumentDB

Puede restaurar una instantánea de un clúster de Amazon DocumentDB para utilizarla como punto de partida del clúster global. Para ello, debe restaurar la instantánea y crear un nuevo clúster. Servirá

como el clúster principal de su clúster global. A continuación, añada otra región al clúster restaurado, convirtiéndolo así en clúster global.

Administración de un clúster global de Amazon DocumentDB

Puede realizar la mayor parte de las operaciones de administración en los clústeres individuales que componen un clúster global. Cuando selecciona Recursos relacionados con grupos en la página Clústeres de la consola, verá el clúster primario y los clústeres secundarios agrupados bajo el objeto de clúster global asociado.

La pestaña Configuración de un clúster global muestra Regiones de AWS dónde se ejecutan los clústeres, la versión y el identificador del clúster global.

Temas

- Modificación de un clúster global de Amazon DocumentDB
- Modificación de los parámetros de un clúster global de Amazon DocumentDB
- Eliminación de un clúster global de Amazon DocumentDB
- Eliminación de un clúster global de Amazon DocumentDB
- Creación de un clúster de Amazon DocumentDB sin pantalla en una región secundaria

Modificación de un clúster global de Amazon DocumentDB

La página Clústeres de la Consola de administración de AWS lista incluye todos los clústeres globales y muestra el clúster principal y los clústeres secundarios de cada uno. El clúster global tiene sus propias opciones de configuración. Específicamente, tiene regiones de asociadas con sus clústeres principal y secundario.

Al realizar cambios en el clúster global, tiene la oportunidad de cancelar los cambios.

Al seleccionar Continue (Continuar), confirma los cambios.

Modificación de los parámetros de un clúster global de Amazon DocumentDB

Puede configurar los grupos de parámetros de clúster independientemente para cada clúster dentro del clúster global. La mayoría de parámetros funcionan igual que para otros tipos de clústeres de Amazon DocumentDB. Se recomienda mantener la configuración coherente entre todos los clústeres de un clúster global. Esto ayuda a evitar cambios de comportamiento inesperados si se promueve un clúster secundario para que sea el principal.

Por ejemplo, utilice la misma configuración de zonas horarias y conjuntos de caracteres para evitar un comportamiento incoherente si un clúster diferente asume la función del clúster principal.

Eliminación de un clúster global de Amazon DocumentDB

Hay varias situaciones en las que es posible que desee eliminar clústeres de su clúster global. Por ejemplo, es posible que desee quitar un clúster de un clúster global si el clúster principal se degrada o se aísla. A continuación, se convierte en un clúster provisionado independiente que podría utilizarse para crear un nuevo clúster global. Para obtener más información, consulte Ejecución de una conmutación por error manual para un clúster global de Amazon DocumentDB.

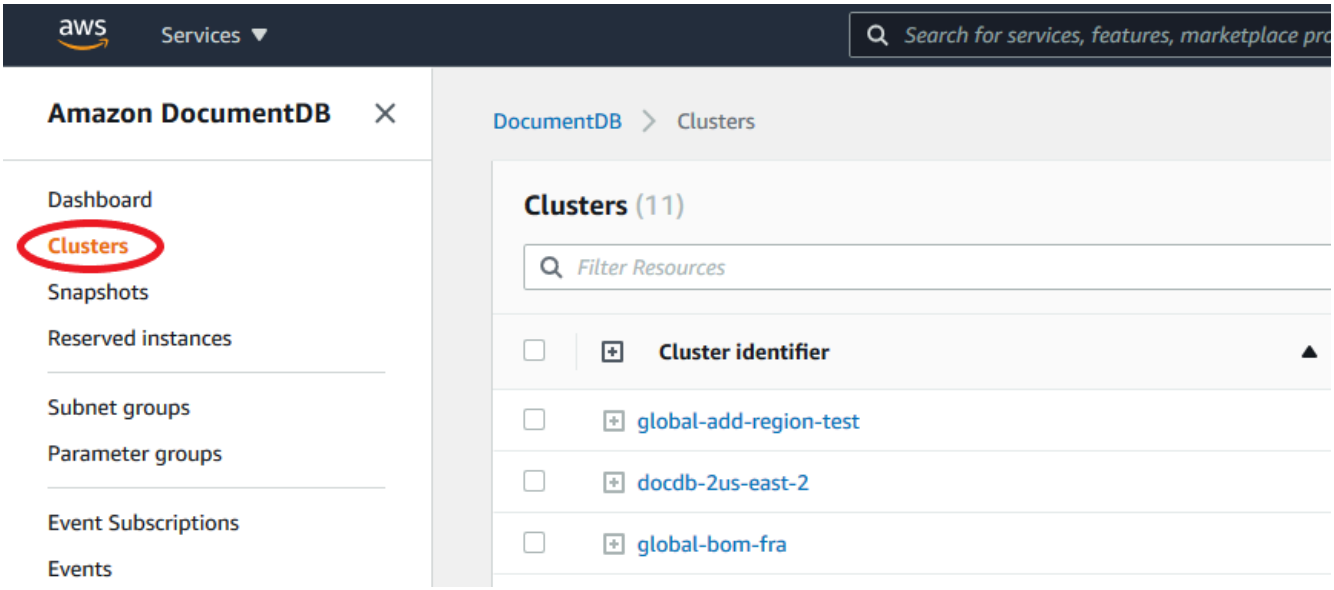
También puede querer quitar clústeres porque desea eliminar un clúster global que ya no necesite. No puede eliminar el clúster global hasta después de eliminar (desasociar) todos los clústeres asociados y deje el principal para lo último. Para obtener más información, consulte Eliminación de un clúster global de Amazon DocumentDB.

> **Note**
>
> Cuando un clúster se desasocia del clúster global, ya no se sincroniza con el principal. Se convierte en un clúster aprovisionado independiente con todas read/write las capacidades. Además, ya no está visible en la consola de Amazon DocumentDB. Solo está visible cuando selecciona la región de la consola en la que estaba ubicado el clúster.

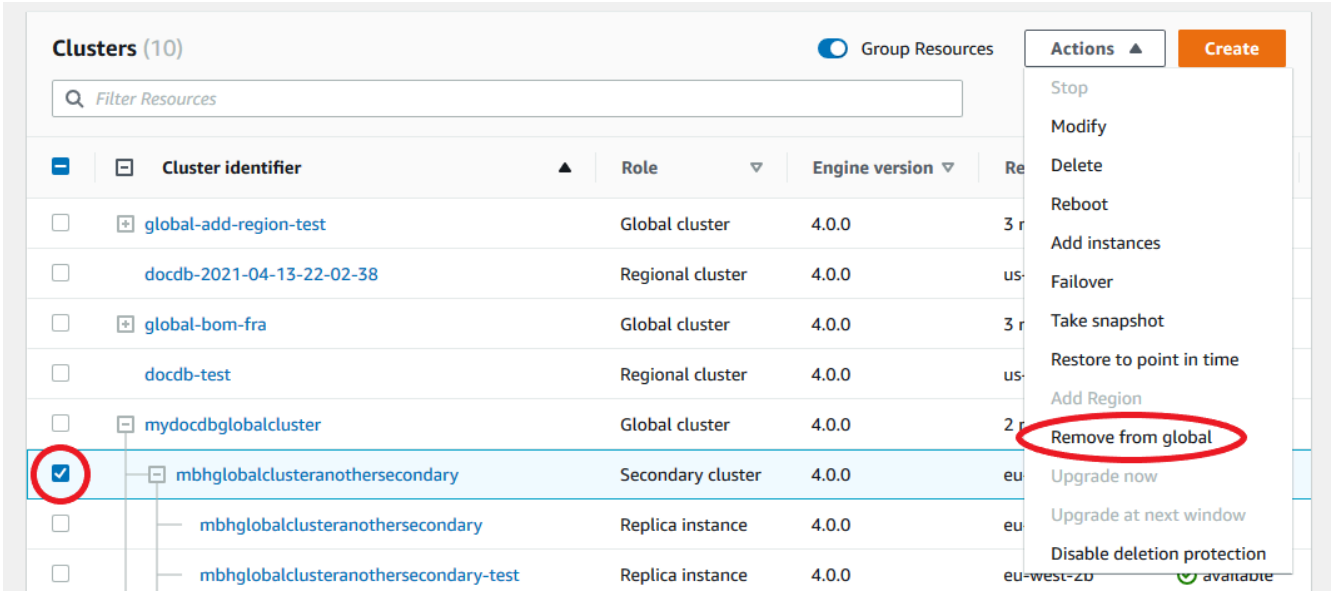
Puede eliminar clústeres de su clúster global mediante la Consola de administración de AWS, la o la AWS CLI API de RDS.

Using the Consola de administración de AWS

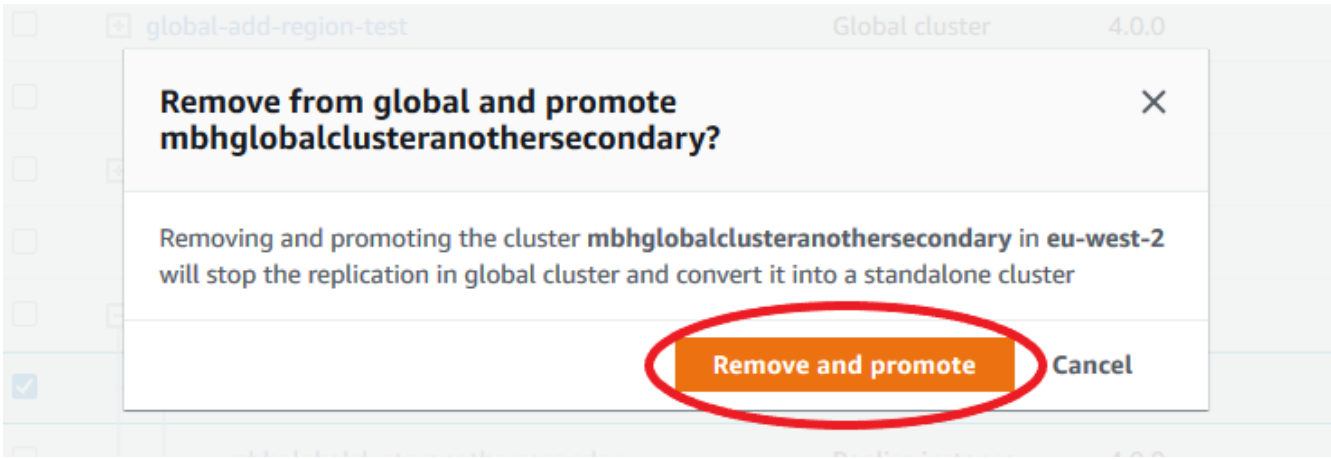
1. Inicie sesión en la consola de Amazon DocumentDB Consola de administración de AWS y navegue hasta ella.
2. En el panel de navegación izquierdo, elija Clústeres.



3. Amplíe el clúster global para que pueda ver todos los clústeres secundarios. Seleccione los clústeres secundarios que desee eliminar. Selecciona Acciones y, en el menú desplegable, selecciona Eliminar del mapa global.



4. Abra un mensaje para confirmar que desea separar el secundario del clúster global. Elija Eliminar y promover para quitar el clúster del clúster global.



El clúster ya no sirve como secundario y ya no está sincronizado con el clúster principal. Se trata de un clúster independiente con capacidad total read/write .

Tras eliminar o borrar todos los clústeres secundarios, podrá eliminar el clúster principal del mismo modo. No puede separar o quitar el clúster principal de un clúster global hasta después de quitar todos los clústeres secundarios. Es posible que el clúster global permanezca en la lista de clústeres, con cero regiones y AZs. Puede eliminar si ya no desea utilizar este clúster global.

Using the AWS CLI

Para eliminar un clúster de un clúster global, ejecute el comando CLI `remove-from-global-cluster` con los siguientes parámetros:

- `--global-cluster-identifier`: nombre (identificador) del clúster global.
- `--db-cluster-identifier`: nombre de cada clúster que se va a quitar del clúster global.

Los siguientes comandos eliminan un clúster secundario y, después, el clúster primario de un clúster global.

Para Linux, macOS o Unix:

```
aws docdb --region secondary_region \
  remove-from-global-cluster \
    --db-cluster-identifier secondary_cluster_ARN \
    --global-cluster-identifier global_cluster_id

aws docdb --region primary_region \
  remove-from-global-cluster \
```

```
    --db-cluster-identifier primary_cluster_ARN \
    --global-cluster-identifier global_cluster_id
```

Repita el comando `remove-from-global-cluster --db-cluster-identifier secondary_cluster_ARN`para cada región secundaria de su clúster global.

Para Windows:

```
aws docdb --region secondary_region ^
  remove-from-global-cluster ^
    --db-cluster-identifier secondary_cluster_ARN ^
    --global-cluster-identifier global_cluster_id

aws docdb --region primary_region ^
  remove-from-global-cluster ^
    --db-cluster-identifier primary_cluster_ARN ^
    --global-cluster-identifier global_cluster_id
```

Repita el comando `remove-from-global-cluster --db-cluster-identifier secondary_cluster_ARN`para cada región secundaria de su clúster global.

Eliminación de un clúster global de Amazon DocumentDB

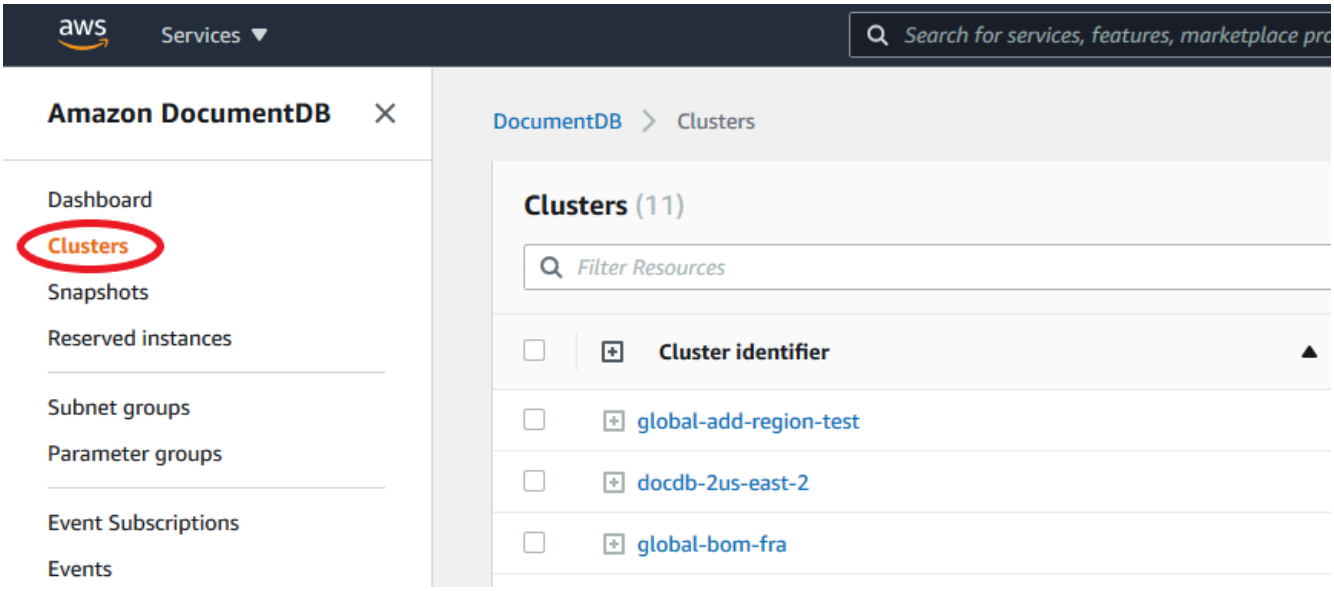
Para completar la eliminación de un clúster global, siga estos pasos:

- Elimine todas las regiones secundarias del clúster global. Cada clúster se convierte en un clúster independiente. Consulte la sección anterior,Eliminación de un clúster global de Amazon DocumentDB.
- En cada clúster independiente, elimine todas las réplicas.
- Elimine el clúster secundario del clúster global. Esto se convierte en un clúster independiente.
- Desde el clúster principal, primero elimine todas las réplicas y, a continuación, elimine la instancia primaria. La eliminación de la instancia de escritor del clúster recién independiente también normalmente elimina el clúster y el clúster global.

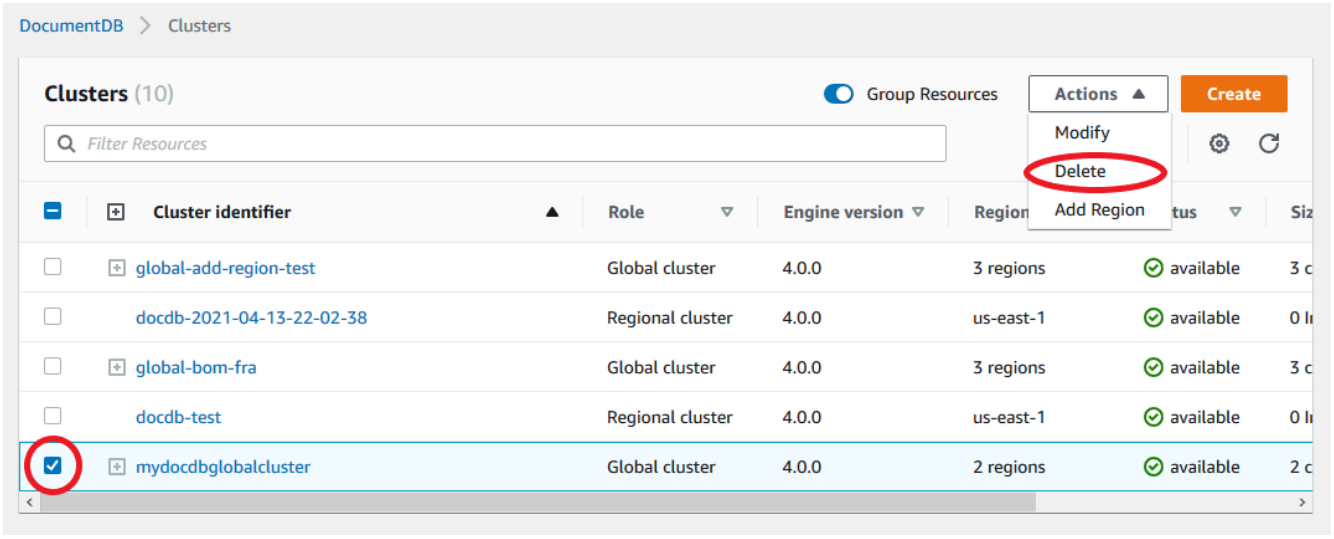
Using the Consola de administración de AWS

1. Inicie sesión en la consola de Amazon DocumentDB Consola de administración de AWS y navegue hasta ella.

2. Elija Clústeres y busque el clúster global que desea eliminar.



3. Con el clúster global seleccionado, selecciona Eliminar en el menú Acciones.



Confirme que todos los demás clústeres se han borrado del clúster global. El clúster global debe mostrar cero regiones AZs y un tamaño igual a cero clústeres. Si el clúster global contiene clústeres, no puede eliminarla. Primero tendrá que seguir las instrucciones del paso anterior, Eliminación de un clúster global de Amazon DocumentDB.

Using the AWS CLI

Para eliminar un clúster global, ejecute el comando `delete-global-cluster` CLI con el nombre Región de AWS y el identificador del clúster global, como se muestra en el siguiente ejemplo.

Para Linux, macOS o Unix:

```
aws docdb --region primary_region delete-global-cluster \
   --global-cluster-identifier global_cluster_id
```

Para Windows:

```
aws docdb --region primary_region delete-global-cluster ^
   --global-cluster-identifier global_cluster_id
```

Creación de un clúster de Amazon DocumentDB sin pantalla en una región secundaria

Si bien un clúster global de Amazon DocumentDB requiere al menos un clúster secundario Región de AWS distinto del principal, puede usar una configuración headless para el clúster secundario. Un clúster secundario de Amazon DocumentDB sin pantalla es uno sin una instancia. Este tipo de configuración puede reducir los gastos para un clúster global. En un clúster de Amazon DocumentDB, se desacoplan la informática y el almacenamiento. Sin la instancia, no se le cobrará por la informática, solo por almacenamiento. Si está configurado correctamente, el volumen de almacenamiento de un clúster secundario sin pantalla se mantiene sincronizado con el clúster principal.

Agregue el clúster secundario como lo hace normalmente al crear un clúster global de Amazon DocumentDB. Sin embargo, después de que el clúster principal comience la reproducción en el secundario, se elimina la instancia de solo lectura del clúster secundario. Ahora, este clúster secundario se considera “sin pantalla” porque ya no tiene una instancia. Sin embargo, el volumen de almacenamiento se mantiene sincronizado con el clúster principal de Amazon DocumentDB.

> **Important**
>
> Solo recomendamos los clústeres headless a los clientes que puedan tolerar errores en toda la región durante más de 15 minutos. Esto se debe a que, para recuperarse de un error en toda la región con un clúster secundario independiente, el usuario tendrá que crear una nueva instancia tras la conmutación por error. Una nueva instancia puede tardar entre 10 y 15 minutos en estar disponible.

Cómo agregar un clúster secundario sin pantalla a su clúster global

1. Inicie sesión en la consola de Amazon DocumentDB Consola de administración de AWS y ábrala.
2. En el panel de navegación izquierdo, elija Clústeres.
3. Elija el clúster global que necesita un clúster secundario. Asegúrese de que el clúster principal es.`Available`
4. En Actions (Acciones), elija Add region (Añadir región).
5. En la página Añadir una región, seleccione la región secundaria.

   > **Note**
   >
   > No puede elegir una región que ya tenga un clúster secundario para el mismo clúster global. Además, no puede ser la misma región que el clúster principal.

6. Complete los campos restantes para el clúster secundario de en la nueva región de. Estas son las mismas opciones de configuración que para cualquier instancia de clúster.
7. Agregar región. Después de terminar de agregar la región al clúster global, puede verla en la lista de`Clusters` de la Consola de administración de AWS.
8. Compruebe el estado del clúster secundario y de su instancia de lectura antes de continuar, utilizando el Consola de administración de AWS o el AWS CLI. A continuación, se muestra un ejemplo de comando si usa la AWS CLI:

   ```
   $ aws docdb describe-db-clusters --db-cluster-identifier secondary-cluster-id --
   query '*[].[Status]' --output text
   ```

   El estado de un clúster secundario recién agregado puede tardar varios minutos en cambiar de “creación en curso” a “disponible”. Cuando el clúster se encuentra disponible, puede eliminar la instancia de lector.
9. Seleccione la instancia de lector en el clúster secundario y, a continuación, elija Eliminar.
10. Después de eliminar la instancia de lector, el clúster secundario sigue siendo parte del clúster global. No debe tener ninguna instancia asociada con él.

> **Note**
>
> Puede utilizar este clúster secundario de Amazon DocumentDB sin pantalla para recuperar manualmente su clúster global de Amazon DocumentDB de una interrupción no planificada en la región principal si se produce una interrupción de este tipo.

Conexión a un clúster global de Amazon DocumentDB

La forma de conectarse a un clúster global depende de si necesita escribir en el clúster o leer del clúster:

- Para solicitudes o consultas de solo lectura, debe conectarse al punto de conexión del lector para el clúster en Región de AWS.
- Para ejecutar instrucciones en lenguaje de manipulación de datos (DML) o lenguaje de definición de datos (DDL), conecte el punto de conexión del clúster para el clúster principal. Es posible que este punto final esté en un lugar Región de AWS diferente al de su aplicación.

Cuando visualice un clúster global en la consola, podrá ver todos los puntos de conexión de uso general asociados a todos sus clústeres.

La forma de conectarse a un clúster global depende de si necesita escribir en la base de datos o leer de ella. Para las operaciones de DDL, DML y lectura que desee realizar desde la región principal, debe conectarse a su clúster primario. Le recomendamos que se conecte a su clúster primario utilizando el punto de conexión del clúster en modo de conjunto de réplicas, con una preferencia de lectura de `secondaryPreferred=true`. Esto redirigirá el tráfico de escritura a la instancia de escritor del clúster primario y el tráfico de lectura a la instancia de réplica del clúster primario.

Para el tráfico de solo lectura entre regiones, debe conectarse a uno de sus clústeres secundarios. Le recomendamos que se conecte a su clúster secundario mediante el punto de conexión del clúster en modo de conjunto de réplicas. Como todas las instancias son réplicas de solo lectura, no es necesario especificar una preferencia de lectura. Para minimizar la latencia, elija el punto de conexión del lector en su región o en la región que tenga más cerca.

Supervisión de clústeres globales de Amazon DocumentDB

Amazon DocumentDB (compatible con MongoDB) se integra CloudWatch para que pueda recopilar y analizar las métricas operativas de sus clústeres. Puede supervisar estas métricas mediante la

CloudWatch consola, la consola Amazon DocumentDB, AWS Command Line Interface (AWS CLI) o la CloudWatch API.

Para monitorear un clúster global, utilice las siguientes CloudWatch métricas.

Métrica	Description (Descripción)
`GlobalClusterReplicatedWriteIO`	El número medio de I/O operaciones de escritura facturadas que se replican desde el volumen del clúster en el principal Región de AWS hasta el volumen del clúster en el secundario Región de AWS, y se informa a intervalos de 5 minutos. El número de réplicas de `ReplicatedWriteIOs` de cada región secundaria es el mismo que el número de `VolumeWriteIOPs` en región realizadas por la región principal.
`GlobalClusterDataTransferBytes`	La cantidad de datos transferidos del clúster principal Región de AWS al clúster secundario Región de AWS, medida en bytes.
`GlobalClusterReplicationLag`	La cantidad de retraso, en milisegundos, al replicar los eventos de cambio del clúster principal Región de AWS a un clúster secundari o Región de AWS

Para obtener más información sobre cómo ver estas métricas, consulta Visualización de CloudWatch datos.

Recuperación ante desastres y clústeres globales de Amazon DocumentDB

Temas

- Ejecución de una conmutación por error administrada para un clúster global de Amazon DocumentDB
- Ejecución de una conmutación por error manual para un clúster global de Amazon DocumentDB
- Ejecución de una transición para un clúster global de Amazon DocumentDB

- Desbloqueo de una conmutación por error o una transición de clúster global

Al utilizar un clúster global, puede recuperarse rápidamente de desastres como errores de región. La recuperación de desastres suele medirse mediante valores para RTO y RPO.

- Objetivo de tiempo de recuperación (RTO) – El tiempo que tarda un sistema en volver a un estado operativo después de un desastre. En otras palabras, el RTO mide el tiempo de inactividad. Para un clúster global, RTO en minutos.
- Objetivo de punto de recuperación (RPO) – La cantidad de datos que se pueden perder (medidos en el tiempo). Para un clúster global, el RPO suele medirse en segundos.
- Para recuperarse de una interrupción imprevista, puede realizar una conmutación por error entre regiones en uno de los secundarios de su clúster global. Cuando su clúster global tenga varias regiones secundarias, asegúrese de separar todas las regiones secundarias que desea promover a primarias. Después, promocione una de esas regiones secundarias para que sea la nueva Región de AWS principal. Por último, creará nuevos clústeres en cada una de las demás regiones secundarias y adjuntará esos clústeres a su clúster global.

Ejecución de una conmutación por error administrada para un clúster global de Amazon DocumentDB

Este enfoque tiene por objeto garantizar la continuidad empresarial en caso de que se produzca un verdadero desastre regional o una interrupción total del nivel de servicio.

Durante una conmutación por error administrada, el clúster principal se conmuta por error a la región secundaria que elija mientras se mantiene la topología de reproducción existente del clúster global de Amazon DocumentDB. El clúster secundario elegido promueve uno de sus nodos de solo de lectura al estado de escritor completo. Este paso permite que el clúster asuma el rol de clúster principal. La base de datos no estará disponible durante un breve periodo, mientras el clúster asume su nuevo rol. Los datos que no se replicaron del clúster principal anterior al clúster secundario elegido se pueden perder cuando este clúster secundario se convierta en el nuevo clúster principal. El volumen principal anterior hace todo lo posible por tomar una instantánea antes de sincronizarla con el nuevo volumen principal, de modo que los datos no replicados se conserven en la instantánea.

> **Note**
>
> Solo puede hacer una conmutación por error administrada del clúster entre regiones en un clúster global de Amazon DocumentDB si el clúster principal y todos los clústeres secundarios tienen las mismas versiones del motor. Si las versiones del motor no son compatibles, puede realizar la conmutación por error manualmente por medio de los pasos que se indican en Ejecución de una conmutación por error manual para un clúster global de Amazon DocumentDB.
>
> Si las versiones del motor de la región no coinciden, se bloqueará la conmutación por error Compruebe si hay actualizaciones pendientes y aplíquelas para garantizar que todas las versiones de motores de la región coincidan y que la conmutación por error global del clúster esté desbloqueada. Para obtener más información, consulte Desbloqueo de una conmutación por error o una transición de clúster global.

Para minimizar la pérdida de datos, le recomendamos que haga lo siguiente antes de utilizar esta característica:

- Desconecte las aplicaciones para evitar que se envíen escrituras al clúster principal del clúster global de Amazon DocumentDB.
- Compruebe los tiempos de retraso para todos los clústeres secundarios de Amazon DocumentDB. La elección de la región secundaria con el menor retraso de replicación puede minimizar la pérdida de datos con respecto a la región principal que actualmente presenta errores. Compruebe los tiempos de retraso de todos los clústeres secundarios de Amazon DocumentDB del clúster global consultando la `GlobalClusterReplicationLag` métrica en Amazon. CloudWatch Estas métricas muestran el retraso (en milisegundos) de la replicación a un clúster secundario con respecto al clúster principal.

  Para obtener más información sobre CloudWatch las métricas de Amazon DocumentDB, consulte. Métricas de Amazon DocumentDB

Durante una conmutación por error administrada, el clúster secundario elegido se promueve a su nuevo rol de clúster principal. Sin embargo, no hereda las diversas opciones de configuración del clúster principal. Una falta de coincidencia en la configuración puede provocar problemas de rendimiento, incompatibilidades de carga de trabajo y otros comportamientos anómalos. Para evitar estos problemas, recomendamos que se resuelvan las diferencias entre los clústeres globales de Amazon DocumentDB para lo siguiente:

- Configure un grupo de parámetros de clúster de Amazon DocumentDB para el nuevo clúster principal, si es necesario: puede configurar los grupos de parámetros de clúster de Amazon DocumentDB de forma independiente para cada clúster del clúster global de Amazon DocumentDB. Por lo tanto, cuando se promueve un clúster secundario para que asuma el rol principal, su grupo de parámetros puede configurarse de manera diferente que para el principal. Si es así, modifique el grupo de parámetros del clúster secundario promocionado para que se ajuste a la configuración del clúster principal. Para aprender a hacerlo, consulte Modificación de grupos de parámetros de clúster de Amazon DocumentDB.
- Configure las herramientas y opciones de monitoreo, como CloudWatch los eventos y las alarmas de Amazon: configure el clúster promocionado con la misma capacidad de registro, alarmas, etc., según sea necesario para el clúster global. Al igual que con los grupos de parámetros, la configuración de estas características no se hereda del clúster principal durante el proceso de conmutación por error. Algunas CloudWatch métricas, como el retraso en la replicación, solo están disponibles para las regiones secundarias. Por lo tanto, una conmutación por error cambia la forma de ver esas métricas y configurar las alarmas en ellas, y podría requerir cambios en los paneles predefinidos. Para obtener más información sobre los clústeres de Amazon DocumentDB y la supervisión, consulte Monitorización de Amazon DocumentDB.

Por lo general, el clúster secundario elegido asume el rol principal en menos de un minuto. En cuanto el nodo de escritor de la nueva región principal esté disponible, podrá conectar sus aplicaciones a él y reanudar sus cargas de trabajo. Una vez que Amazon DocumentDB promueve el nuevo clúster principal, reconstruye automáticamente todos los clústeres regionales secundarios adicionales.

Como los clústeres globales de Amazon DocumentDB utilizan la replicación asíncrona, el retraso de la replicación en cada región secundaria puede variar. Amazon DocumentDB reconstruye estas regiones secundarias para que tengan exactamente los mismos point-in-time datos que el nuevo clúster de regiones principal. La duración de la tarea de reconstrucción completa puede tardar entre unos minutos y varias horas, según el tamaño del volumen de almacenamiento y la distancia entre las regiones. Cuando los clústeres de la región secundaria terminen de reconstruirse a partir de la nueva región principal, estarán disponibles para el acceso de lectura. Tan pronto como se promocione y esté disponible el nuevo escritor principal, el clúster de la nueva región principal podrá gestionar las operaciones de lectura y escritura del clúster global de Amazon DocumentDB.

Para restaurar la topología original del clúster global, Amazon DocumentDB supervisa la disponibilidad de la antigua región principal. Tan pronto como la región esté en buen estado y vuelva a estar disponible, Amazon DocumentDB volverá a agregarla automáticamente al clúster global como región secundaria. Antes de crear el nuevo volumen de almacenamiento en la

antigua región principal, Amazon DocumentDB intenta tomar una instantánea del volumen de almacenamiento anterior en el punto en que se produjo el error. Lo hace para que pueda usarla para recuperar cualquiera de los datos perdidos. Si la operación se realiza correctamente, Amazon DocumentDB coloca esta instantánea denominada «rds: docdb-unplanned-global-failover - name-of-old-primary -DB-Cluster-Timestamp» en la sección de instantáneas del. Consola de administración de AWS También puede ver esta instantánea en la información devuelta por la operación de la API `DescribeDBClusterSnapshots`.

> **Note**
>
> La instantánea del volumen de almacenamiento anterior es una instantánea del sistema que está sujeta al período de retención de la copia de seguridad configurado en el clúster principal anterior. Para conservar esta instantánea más allá del período de retención, puede copiarla para guardarla como una instantánea manual. Para obtener más información sobre la copia de instantáneas, incluido el precio, consulte Copia de una instantánea de clúster.

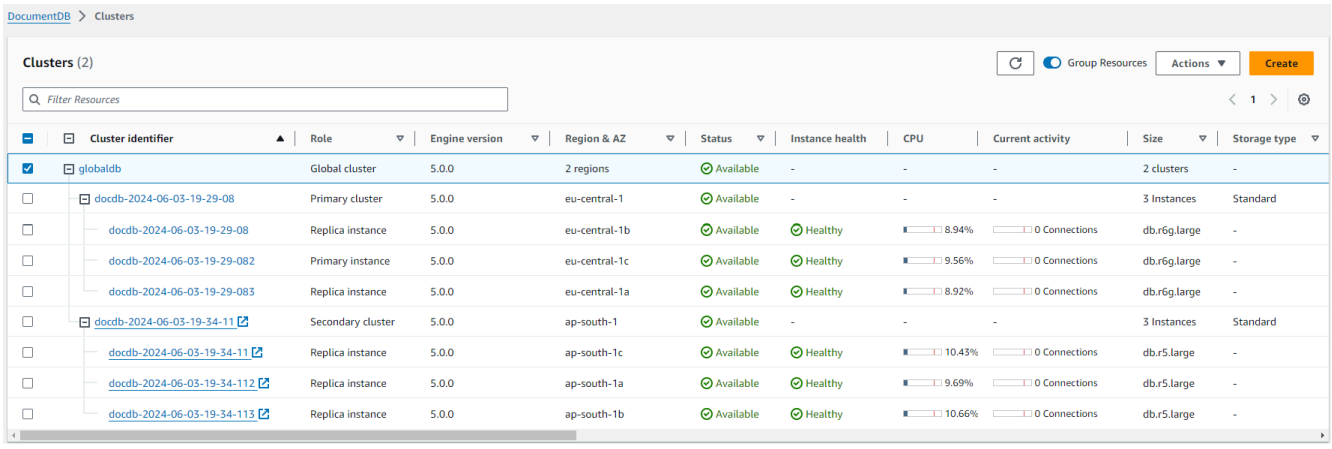
Una vez restaurada la topología original, puede conmutar por recuperación el clúster global a la región principal original mediante una operación de transición cuando sea más conveniente para su empresa y su carga de trabajo. Para ello, siga los pasos que se indican en Ejecución de una transición para un clúster global de Amazon DocumentDB.

Puede realizar una conmutación por error de su clúster global de Amazon DocumentDB mediante la Consola de administración de AWS, la o la AWS CLI API de Amazon DocumentDB.

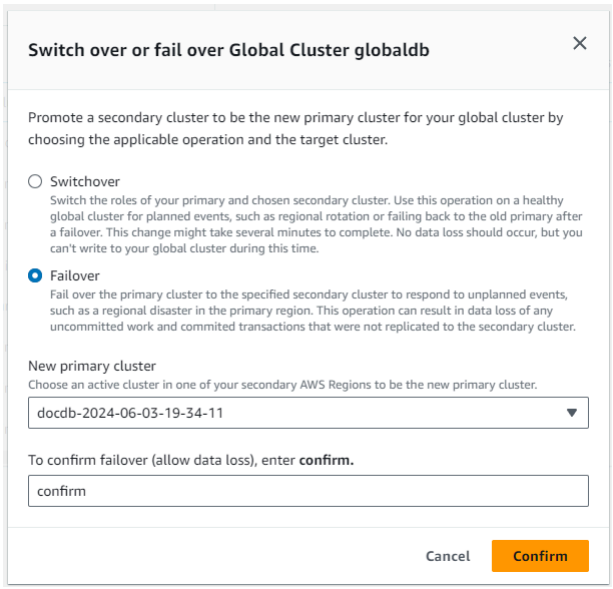
Using the Consola de administración de AWS

Ejecución de una conmutación por error administrada en el clúster global de Amazon DocumentDB

1. Inicie sesión en y abra la Consola de administración de AWS consola de Amazon DocumentDB en https://console.aws.amazon.com /docdb.
2. En el panel de navegación, seleccione Clusters (Clústeres).
3. Busque y elija el clúster global de Amazon DocumentDB que desea someter al proceso de conmutación por error.



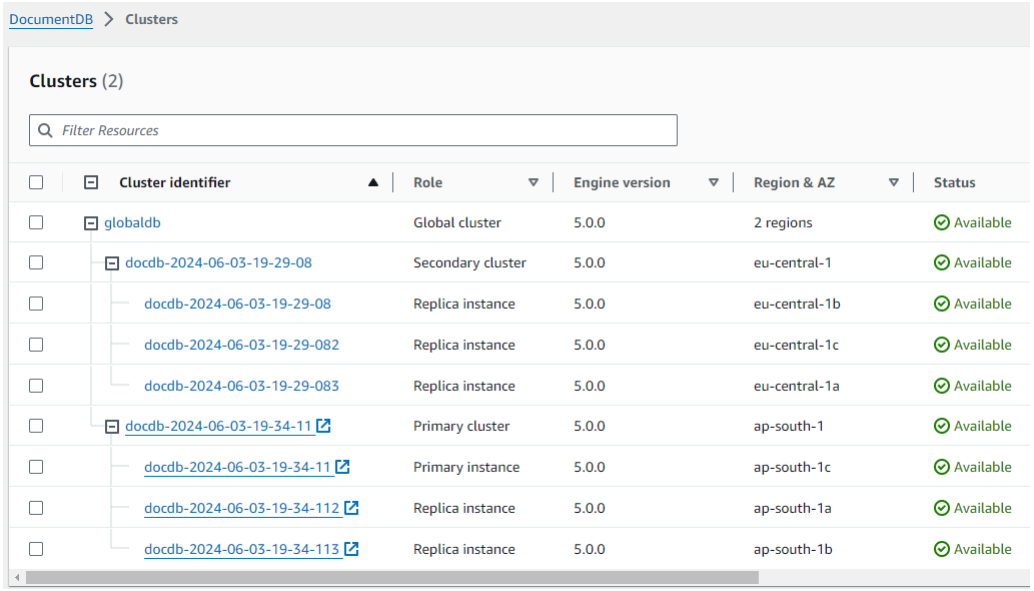
4. Elija Transición o conmutación por error en el menú Acciones.
5. En el cuadro de diálogo que aparece, seleccione Conmutación por error y, a continuación, elija el clúster secundario en la lista desplegable del campo Nuevo clúster principal.



6. Escriba “confirmar” en el último campo. A continuación, seleccione Confirm (Confirmar).

   El estado del clúster principal cambia a “Conmutación por error”. Esta condición puede necesitar aproximadamente un minuto. Durante este tiempo, el estado del nuevo clúster principal muestra “Modificando…”. Una vez que se promocione el nuevo clúster principal, aparecerá como “Disponible” y podrá procesar transacciones de lectura y escritura. Las regiones secundarias, incluida la antigua principal, mostrarán el mensaje “Resincronizando…” mientras se vuelve a sincronizar con el nuevo clúster principal. Al igual que el nuevo clúster principal, solo podrá procesar transacciones una vez que su estado cambie a “Disponible”.

7. Cuando se complete, el clúster principal original se convierte en el clúster secundario. El clúster secundario seleccionado se convierte en el clúster principal.



Using the AWS CLI

Ejecución de una conmutación por error administrada en el clúster global de Amazon DocumentDB

Ejecute el comando `failover-global-cluster` de la CLI para conmutar por error el clúster global de Amazon DocumentDB. Con el comando, pase valores para las siguientes opciones:

- `--region`
- `--global-cluster-identifier`
- `--target-db-cluster-identifier`
- `--allow-data-loss`

En los siguientes ejemplos, sustituya cada uno por la información *`user input placeholder`* de su clúster.

Para Linux, macOS o Unix:

```
aws docdb failover-global-cluster \
   --region region_of_selected_secondary \
   --global-cluster-identifier global_cluster_id \
   --target-db-cluster-identifier arn_of_secondary_to_promote \
```

```
    --allow-data-loss
```

Para Windows:

```
aws docdb failover-global-cluster ^
   --region region_of_selected_secondary ^
   --global-cluster-identifier global_cluster_id ^
   --target-db-cluster-identifier arn_of_secondary_to_promote ^
   --allow-data-loss
```

Ejecución de una conmutación por error manual para un clúster global de Amazon DocumentDB

Si un clúster completo de uno Región de AWS deja de estar disponible, puedes promover otro clúster del clúster global para que tenga esa read/write capacidad.

Puede activar manualmente el mecanismo de conmutación por error del clúster global si un clúster de una Región de AWS diferente es una mejor opción para ser el clúster primario. Por ejemplo, puede aumentar la capacidad de uno de esos clústeres secundarios y promoverlo para que sea el clúster principal. O bien, el equilibrio de la actividad entre ellos Regiones de AWS podría cambiar, por lo que cambiar el clúster principal a otro Región de AWS podría reducir la latencia de las operaciones de escritura.

El siguiente procedimiento describe qué hacer para promocionar uno de los clústeres secundarios de un clúster global de Amazon DocumentDB.

Para promover un clúster secundario:

1. Tras la interrupción, deje de emitir sentencias DML y otras operaciones de escritura en el Región de AWS clúster principal.
2. Identifique un clúster de un secundario Región de AWS para usarlo como un nuevo clúster principal. Si tiene dos (o más) secundarios Regiones de AWS en su clúster global, elija el clúster secundario que tenga el menor tiempo de retraso.
3. Desconecte el clúster secundario del clúster global elegido.

   Al eliminar un clúster secundario de un clúster global, se detiene inmediatamente la replicación del clúster principal a este secundario y se convierte en un clúster aprovisionado independiente con todas read/write las capacidades. Todavía está disponible cualquier otro clúster secundario

asociado con el clúster primario de la región con la interrupción y puede aceptar llamadas desde la aplicación. También consumen recursos. Dado que está recreando el clúster global, para evitar problemas de split-brain y otros problemas, elimine los otros clústeres secundarios antes de crear el nuevo clúster en los pasos que se indican a continuación.

Para obtener más información sobre los pasos para desasociar clústeres, consulte Eliminación de un clúster global de Amazon DocumentDB.

4. Este clúster se convierte en el clúster primario de un nuevo clúster global cuando comienza a agregarle regiones, en el siguiente paso.
5. Agregue un elemento Región de AWS al clúster. Al hacerlo, comienza el proceso de reproducción de clúster principal a secundario.
6. Agregue más Regiones de AWS según sea necesario para volver a crear la topología necesaria para respaldar su aplicación. Asegúrese de que las escrituras de la aplicación se envían al clúster correcto antes, durante y después de realizar cambios como estos, para evitar incoherencias de datos entre los clústeres en el clúster global (problemas de split-brain).
7. Cuando se haya resuelto la interrupción y esté listo para asignar su Región de AWS original como clúster primario de nuevo, realice los mismos pasos en orden inverso.
8. Elimine uno de los clústeres secundarios del clúster global. Esto le permitirá atender read/write el tráfico.
9. Redirija todo el tráfico de escritura del clúster primario en la Región de AWS original.
10. Agregue un Región de AWS para configurar uno o más clústeres secundarios de la Región de AWS misma manera que antes.

Los clústeres globales de Amazon DocumentDB se pueden administrar mediante AWS SDKs, lo que le permite crear soluciones para automatizar el proceso de conmutación por error de clústeres globales para casos de uso de recuperación ante desastres y planificación de la continuidad empresarial. Una de estas soluciones está disponible para nuestros clientes con las licencias de Apache 2.0 y se puede acceder a ella desde nuestro repositorio de herramientas aquí. Esta solución aprovecha Amazon Route 53 para la administración de puntos finales y proporciona AWS Lambda funciones que se pueden activar en función de los eventos apropiados.

Ejecución de una transición para un clúster global de Amazon DocumentDB

Al utilizar las transiciones, puede cambiar la región del clúster principal de forma rutinaria. Este enfoque está destinado a situaciones controladas, como el mantenimiento operativo y otros procedimientos operativos planificados.

Existen tres casos de uso frecuentes en los que se utilizan las transiciones:

- Para los requisitos de “rotación regional” impuestos a sectores específicos. Por ejemplo, es posible que los reglamentos de los servicios financieros exijan que los sistemas de nivel 0 se cambien a una región diferente durante varios meses para garantizar que los procedimientos de recuperación de desastres se ensayen con cierta asiduidad.
- Para aplicaciones «follow-the-sun» multirregionales. Por ejemplo, es posible que una empresa desee ofrecer escrituras con menor latencia en diferentes regiones en función del horario laboral en distintas zonas horarias.
- Como zero-data-loss método para volver a la región principal original tras una conmutación por error.

> **Note**
>
> Las transiciones están diseñadas para utilizarse en un clúster global de Amazon DocumentDB en buen estado. Para la recuperación de una interrupción no programada, siga el procedimiento correspondiente en Ejecución de una conmutación por error manual para un clúster global de Amazon DocumentDB.
>
> Para realizar una transición, todas las regiones secundarias deben ejecutar la misma versión del motor que la versión principal. Si las versiones del motor de la región no coinciden, se bloqueará la transición. Compruebe si hay actualizaciones pendientes y aplíquelas para garantizar que todas las versiones de motores de la región coincidan y que la transición global del clúster esté desbloqueada. Para obtener más información, consulte Desbloqueo de una conmutación por error o una transición de clúster global.

Durante una transición, Amazon DocumentDB cambia el clúster principal a la región secundaria que elija a la vez que mantiene la topología de replicación existente del clúster global. Antes de iniciar el proceso de transición, Amazon DocumentDB espera a que todos los clústeres de regiones secundarias estén completamente sincronizados con el clúster de la región principal. A continuación, el clúster de bases de datos de la región principal se convierte en un clúster de solo lectura y el clúster secundario que elija promueve uno de sus nodos de solo lectura a estado de escritor completo. Al convertir este nodo en escritor, el clúster secundario puede asumir el rol de clúster principal. Dado que todos los clústeres secundarios se sincronizaron con el principal al principio del proceso, el nuevo principal continúa las operaciones para el clúster global de Amazon DocumentDB

sin perder ningún dato. La base de datos no estará disponible durante un breve periodo, mientras los clústeres principales y secundarios seleccionados asumen nuevas funciones.

Para optimizar la disponibilidad de las aplicaciones, se recomienda hacer lo siguiente antes de utilizar esta característica:

- Lleve a cabo esta operación durante los horarios menos concurridos o en otro momento cuando las escrituras en el clúster principal sean mínimas.
- Desconecte las aplicaciones para evitar que se envíen escrituras al clúster principal del clúster global de Amazon DocumentDB.
- Compruebe los tiempos de retraso de todos los clústeres secundarios de Amazon DocumentDB del clúster global consultando la `GlobalClusterReplicationLag` métrica en Amazon. CloudWatch Esta métrica muestra el retraso (en milisegundos) de la replicación a un clúster secundario con respecto al clúster principal. Este valor es directamente proporcional al tiempo que tarda Amazon DocumentDB en completar la transición. Por lo tanto, cuanto mayor sea el valor de retraso, más tiempo llevará la transición.

  Para obtener más información sobre CloudWatch las métricas de Amazon DocumentDB, consulte. Métricas de Amazon DocumentDB

Durante una transición, el clúster secundario de base de datos elegido se promueve a su nuevo rol de clúster principal. Sin embargo, no hereda las diversas opciones de configuración del clúster principal de base de datos. Una falta de coincidencia en la configuración puede provocar problemas de rendimiento, incompatibilidades de carga de trabajo y otros comportamientos anómalos. Para evitar estos problemas, recomendamos que se resuelvan las diferencias entre los clústeres globales de Amazon DocumentDB para lo siguiente:

- Configure un grupo de parámetros de clúster de base de datos de Amazon DocumentDB para el nuevo clúster principal, si es necesario: puede configurar los grupos de parámetros de clúster de Amazon DocumentDB de forma independiente para cada clúster del clúster global de Amazon DocumentDB. Esto significa que cuando se promueve un clúster secundario de base de datos para asumir el rol principal, su grupo de parámetros puede configurarse de manera diferente que para el principal. Si es así, modifique el grupo de parámetros del clúster secundario de base de datos promocionado para que se ajuste a la configuración del clúster principal. Para saber cómo hacerlo, consulte Administración de los grupos de parámetros de clúster de Amazon DocumentDB.
- Configure las herramientas y opciones de monitoreo, como Amazon CloudWatch Events y las alarmas: configure el clúster promocionado con la misma capacidad de registro, alarmas,

etc., según sea necesario para el clúster global. Al igual que con los grupos de parámetros, la configuración de estas características no se hereda del clúster principal durante el proceso de transición. Algunas CloudWatch métricas, como el retraso en la replicación, solo están disponibles para las regiones principales. Por lo tanto, una transición cambia la forma de ver esas métricas y configurar las alarmas en ellas, y podría requerir cambios en los paneles predefinidos. Para obtener más información, consulte Monitorización de Amazon DocumentDB.

> **Note**
>
> Por lo general, la transición de rol puede tardar varios minutos.

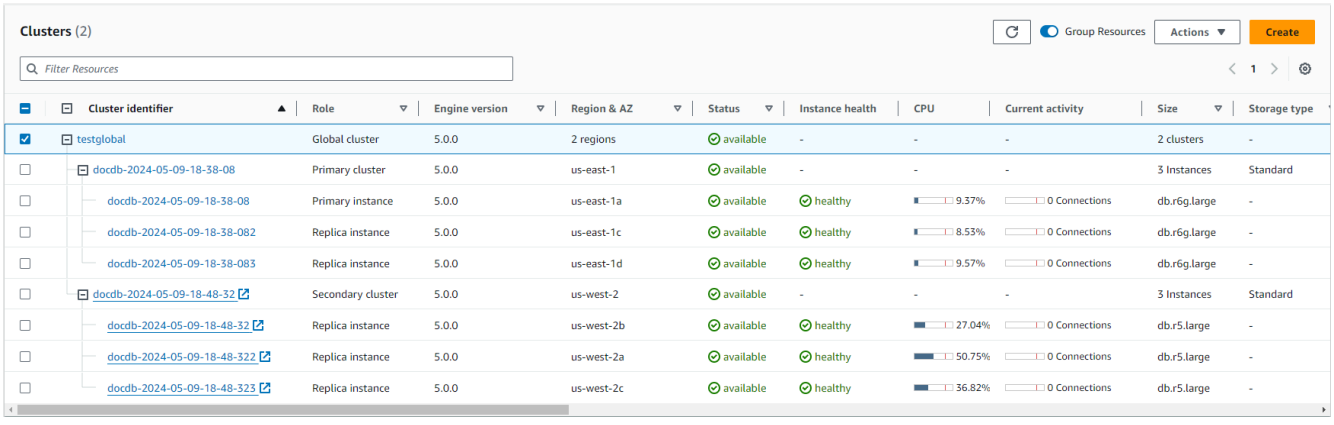
Cuando finaliza el proceso de transición, el clúster de Amazon DocumentDB promocionado puede manejar operaciones de escritura para el clúster global.

Puede cambiar su clúster global de Amazon DocumentDB mediante Consola de administración de AWS o: AWS CLI

Using the Consola de administración de AWS

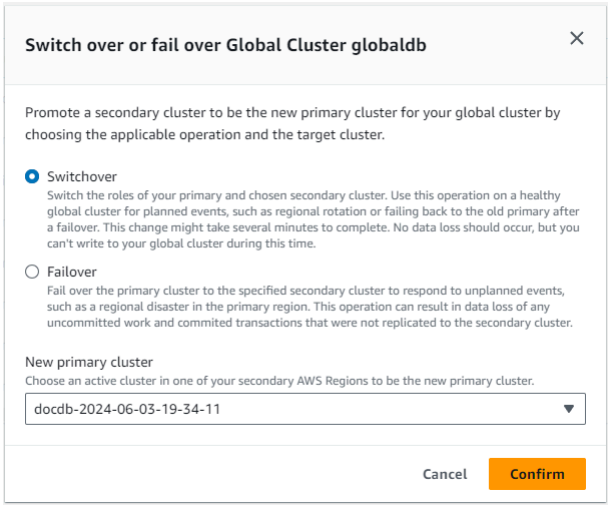
Ejecución de una transición en un clúster global de Amazon DocumentDB

1. Inicie sesión en y abra la Consola de administración de AWS consola de Amazon DocumentDB en https://console.aws.amazon.com /docdb.
2. En el panel de navegación, seleccione Clusters (Clústeres).
3. Busque y elija el clúster global de Amazon DocumentDB que desea someter al proceso de transición.



4. Elija Transición o conmutación por error en el menú Acciones.

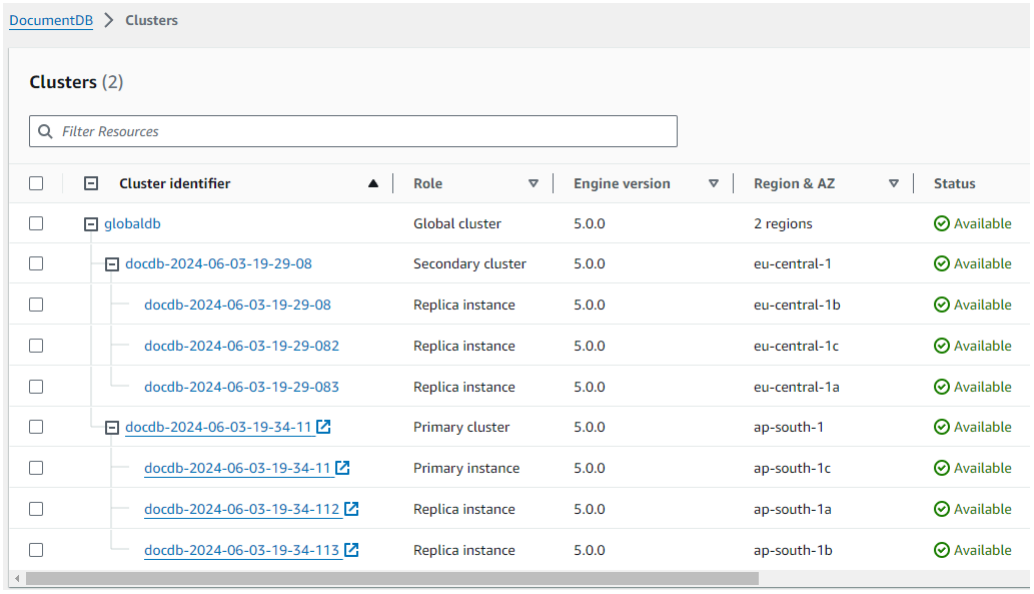
5. En el cuadro de diálogo que aparece, seleccione Transición y, a continuación, elija el clúster secundario en la lista desplegable del campo Nuevo clúster principal.



6. Elija Confirmar.

   El estado del clúster principal cambia a “Transición”. Esta condición puede necesitar aproximadamente tres minutos. Durante este tiempo, el estado de todos los clústeres regionales muestra “Modificando...”. Una vez que las regiones se sincronicen y se promocione el nuevo clúster principal, aparecerá como “Disponible” en todos los campos de estado y podrá procesar transacciones.

7. Cuando se complete, el clúster principal original se convierte en el clúster secundario. El clúster secundario seleccionado se convierte en el clúster principal.



Using the AWS CLI

Ejecución de una transición en un clúster global de Amazon DocumentDB

Utilice el comando `switchover-global-cluster` de la CLI para hacer la transición del clúster global de Amazon DocumentDB. Con el comando, pase valores para las siguientes opciones:

- `--region`
- `--global-cluster-identifier`
- `--target-db-cluster-identifier`

En los siguientes ejemplos, sustituya cada uno por la información *`user input placeholder`* de su clúster.

Para Linux, macOS o Unix:

```
aws docdb switchover-global-cluster \
   --region region_of_primary \
   --global-cluster-identifier global_cluster_id \
   --target-db-cluster-identifier arn_of_secondary_to_promote
```

Para Windows:

```
aws docdb switchover-global-cluster ^
   --region region_of_primary ^
   --global-cluster-identifier global_cluster_id ^
   --target-db-cluster-identifier arn_of_secondary_to_promote
```

Desbloqueo de una conmutación por error o una transición de clúster global

Las transiciones y las conmutaciones por error de clústeres globales se bloquean cuando no todos los clústeres regionales del clúster global están en la misma versión del motor. Si las versiones no coinciden, es posible que aparezca este error como respuesta cuando llama una transición o una conmutación por error: el clúster de base de datos de destino especificado ejecuta una versión de motor con un nivel de parche diferente al del clúster de base de datos de origen. Le recomendamos que aplique de forma rutinaria las últimas versiones del motor para asegurarse de que está ejecutando las actualizaciones más recientes y así mantener sus clústeres globales en buen estado.

Para resolver este error, actualice primero todas las regiones secundarias y, después, la región principal a la misma versión de motor aplicando las medidas de mantenimiento pendientes. Para ver las acciones de mantenimiento pendientes y aplicar los cambios necesarios para corregir el problema, siga las instrucciones de una de las siguientes pestañas:

Using the Consola de administración de AWS

Para desbloquear una transición o conmutación por error de clúster global, debe determinar si hay acciones de mantenimiento pendientes para sus clústeres y aplicarlas. Siga estos pasos para ver y aplicar las acciones de mantenimiento:

1. Inicie sesión en y abra la Consola de administración de AWS consola de Amazon DocumentDB en https://console.aws.amazon.com /docdb.
2. En el panel de navegación, seleccione Clusters (Clústeres).
3. En la tabla Clústeres, localice el clúster global en la columna de Identificador de clúster. En su clúster global, anote cada clúster secundario y el clúster principal del clúster global en cuestión, y realice los siguientes pasos para cada uno.
4. Para cada clúster secundario:
    a. Si hay una actualización disponible para el clúster, se indicará con la palabra Disponible, Obligatorio o Siguiente período en la columna Mantenimiento.
    b. Para realizar una acción, elija el clúster para mostrar sus detalles y, a continuación, seleccione Mantenimiento y copias de seguridad. Aparecerán los elementos de mantenimiento pendientes.
    c. En Descripción, si indica que hay una «Nueva actualización de mantenimiento disponible», selecciónela y, a continuación, elija Aplicar ahora.
5. Para su clúster principal:
    a. Si hay una actualización disponible para el clúster, se indicará con la palabra Disponible, Obligatorio o Siguiente período en la columna Mantenimiento.
    b. Para realizar una acción, elija el clúster para mostrar sus detalles y, a continuación, seleccione Mantenimiento y copias de seguridad. Aparecerán los elementos de mantenimiento pendientes.
    c. En Descripción, si indica que hay una «Nueva actualización de mantenimiento disponible», selecciónela y, a continuación, elija Aplicar ahora.

Using the AWS CLI

Para desbloquear una transición o conmutación por error de clúster global, debe determinar si hay acciones de mantenimiento pendientes para el clúster y aplicarlas. Siga estos pasos para ver y aplicar las acciones de mantenimiento primero en los clústeres secundarios y, después, en el clúster principal del clúster global:

1. Primero ejecute lo siguiente en el clúster regional de cada región secundaria y, a continuación, en el clúster regional de la región principal.
2. Ejecute el comando `describe-pending-maintenance-actions` de la CLI con la opción `--resource-identifier` para determinar si hay acciones de mantenimiento disponibles para su clúster regional de Amazon DocumentDB.

   En los siguientes ejemplos, sustituya cada uno por la información *`user input placeholder`* de su clúster.

   Para Linux, macOS o Unix:

   ```
   aws docdb describe-pending-maintenance-action \
      --resource-identifier arn:aws:rds:us-
   east-1:001234567890:cluster:docdb-2025-03-27-19-21-15
   ```

   Para Windows:

   ```
   aws docdb describe-pending-maintenance-action ^
      --resource-identifier arn:aws:rds:us-
   east-1:001234567890:cluster:docdb-2025-03-27-19-21-15
   ```

   El resultado tendrá un aspecto parecido al siguiente:

   ```
   {
       "PendingMaintenanceActions": [
           {
               "ResourceIdentifier": "arn:aws:rds:us-
   east-1:001234567890:cluster:docdb-2025-03-27-19-21-15",
               "PendingMaintenanceActionDetails": [
                   {
                       "Action": "system-update",
                       "CurrentApplyDate": "2025-04-11T03:01:00Z",
                       "Description": "db-version-upgrade",
   ```

```
                    "ForcedApplyDate": "2025-06-18T03:01:00Z",
                    "AutoAppliedAfterDate": "2025-05-11T03:01:00Z"
                    "OptInStatus": "pending"
                }
            ]
        }
    ]
}
```

3. Si es necesaria una acción de mantenimiento, ejecute el comando [apply-pending-maintenance-action] de la CLI con las siguientes opciones:

   - `--resource-identifier`
   - `--apply-action`
   - `--opt-in-type`
   - `--region`

   En los ejemplos siguientes, sustituya cada uno *`user input placeholder`* por la información de su clúster.

   Para Linux, macOS o Unix:

```
aws docdb apply-pending-maintenance-action \
   --resource-identifier arn:aws:rds:us-
east-1:001234567890:cluster:docdb-2025-03-27-19-21-15 \
   --apply-action system-update \
   --opt-in-type immediate \
   --region us-east-1
```

   Para Windows:

```
aws docdb apply-pending-maintenance-action ^
   --resource-identifier arn:aws:rds:us-
east-1:001234567890:cluster:docdb-2025-03-27-19-21-15 ^
   --apply-action system-update ^
   --opt-in-type immediate ^
   --region us-east-1
```

4. Una vez finalizada la acción de mantenimiento, vuelva a ejecutar el comando `describe-pending-maintenance-actions` para asegurarse de que no haya otras acciones pendientes para el clúster.

   El resultado que desea es:

   ```
   {
       "PendingMaintenanceActions": []
   }
   ```

Using the Amazon DocumentDB API

Para desbloquear una transición o conmutación por error de clúster global, debe determinar si hay acciones de mantenimiento pendientes para el clúster y aplicarlas. Utilice lo siguiente APIs para ver y aplicar las acciones de mantenimiento:

1. Primero ejecute lo siguiente en el clúster regional de cada región secundaria y, a continuación, en el clúster regional de la región principal.
2. Llame a la API de `PendingMaintenanceAction` para determinar si hay acciones de mantenimiento disponibles para su clúster global de Amazon DocumentDB.
3. Para aplicar cualquier cambio, llame a la API de `ApplyPendingMaintenanceAction`.

Administración de clústeres de Amazon DocumentDB

Para administrar un clúster de Amazon DocumentDB, debe disponer de una política de IAM con los permisos del plano de control de Amazon DocumentDB. Estos permisos le permiten crear, modificar y eliminar clústeres e instancias. La política `AmazonDocDBFullAccess` proporciona todos los permisos necesarios para administrar un clúster de Amazon DocumentDB.

Los siguientes temas muestran cómo realizar diversas tareas cuando se trabaja con clústeres de Amazon DocumentDB, incluida la creación, eliminación, modificación, conexión y consulta de clústeres.

Temas

- Descripción de clúster
- Configuración del clúster de Amazon DocumentDB
- Configuraciones de almacenamiento en clústeres de Amazon DocumentDB

- Determinación del estado de un clúster
- Ciclo de vida del clúster de Amazon DocumentDB
- Escalado de clústeres de Amazon DocumentDB
- Clonación de un volumen de clúster de base de datos de Amazon DocumentDB
- Información general de la tolerancia a errores de clúster de Amazon DocumentDB

Descripción de clúster

Amazon DocumentDB divide la capacidad informática y de almacenamiento, y descarga la replicación de datos y las copias de seguridad en el volumen del clúster. Un volumen de clúster proporciona una capa de almacenamiento duradera, fiable y altamente disponible que replica los datos de seis formas distintas entre tres zonas de disponibilidad. Las réplicas permiten una mayor disponibilidad de los datos y del escalado de lectura. Cada clúster se puede escalar hasta 15 réplicas.

Nombre	Description (Descripción)	Operaciones de API (Verbos)

Clúster	Se compone de una o varias instancias y de un volumen de almacenamiento del clúster que administra los datos para esas instancias.	`create-db-cluster`
		`delete-db-cluster`
		`describe-db-clusters`
		`modify-db-cluster`

Instancia	La lectura y escritura de los datos en el volumen de almacenamiento del clúster se realiza a través de las instancias. En cualquier clúster, hay dos tipos de instancias: principal y de réplica. Un clúster siempre tiene una instancia principal y puede tener 0-15 réplicas.	`create-db-instance`
		`delete-db-instance`
		`describe-db-instances`
		`modify-db-instance`
		`describe-orderable-db-instance-options`
		`reboot-db-instance`

Nombre	Description (Descripción)	Operaciones de API (Verbos)
Volumen del clúster	Un volumen de almacenamiento de base de datos virtual que abarca tres zonas de disponibilidad, de modo que cada una de estas zonas tenga dos copias de los datos del clúster.	N/A
Instancia principal	Admite operaciones de lectura y escritura, y realiza todas las modificaciones de los datos en el volumen del clúster. Cada clúster tiene una instancia principal.	N/A
Instancia de réplica	Solo admite operaciones de lectura. Cada clúster de Amazon DocumentDB puede tener hasta 15 instancias de réplica, además de la instancia principal. Varias réplicas distribuyen la carga de trabajo real. Al colocar las réplicas en distintas zonas de disponibilidad, también puede aumentar la disponibilidad de la base de datos.	N/A

Nombre	Description (Descripción)	Operaciones de API (Verbos)
Punto de conexión de clúster	Un punto de conexión de un clúster de Amazon DocumentDB que se conecta a la instancia principal actual del clúster. Cada clúster de Amazon DocumentDB tiene un punto de conexión de clúster y una instancia principal.	N/A
Punto de conexión del lector	Un punto de conexión de un clúster de Amazon DocumentDB que se conecta a una de las réplicas disponibles de ese clúster. Cada clúster de base de datos de Amazon DocumentDB tiene un punto de conexión del lector. Si hay más de una réplica, el punto de conexión del lector dirige cada solicitud de conexión a una de las réplicas de Amazon DocumentDB.	N/A
Punto de conexión de instancia	Un punto de conexión de una instancia de un clúster de Amazon DocumentDB que se conecta a una instancia específica. Cada instancia de un clúster de base de datos, independientemente del tipo de instancia, tiene su propio punto de conexión de instancia único.	N/A

Configuración del clúster de Amazon DocumentDB

Al crear o modificar un clúster, es importante saber qué parámetros son inmutables y cuáles se pueden modificar una vez creado el clúster. La siguiente tabla muestra todas las configuraciones o parámetros que son específicos en un clúster. Tal y como se indica en la tabla; algunos de ellos se pueden modificar y otros no.

> **Note**
>
> Esta configuración no debe confundirse con los grupos de parámetros de clúster de Amazon DocumentDB y sus parámetros. Para obtener más información acerca de los grupos de parámetros de clúster, consulte Administración de los grupos de parámetros de clúster de Amazon DocumentDB.

Parámetro	Modificable	Notas
`DBClusterIdentifier`	Sí	Restricciones en la nomenclatura: • Debe tener [1-63] letras, números o guiones. • El primer carácter debe ser una letra. • No puede terminar con un guion ni contener dos guiones consecutivos. • Debe ser único para todos los clústeres de Amazon RDS, Amazon Neptune y Amazon DocumentDB por región. Cuenta de AWS
`Engine`	No	Debe ser `docdb`.
`BackupRetentionPeriod`	Sí	Debe estar comprendido entre [1-35] días.
`DBClusterParameterGroupName`	Sí	Restricciones en la nomenclatura: • La longitud es de [1-255] caracteres alfanuméricos. • El primer carácter debe ser una letra.

Parámetro	Modificable	Notas
		• No puede terminar con un guion ni contener dos guiones consecutivos.
DBSubnetGroupName	No	Una vez creado un clúster, no puede modificar la subred del clúster.
EngineVersion	No	El valor puede ser `5.0.0` (predeterminado), `4.0.0` o `3.6.0`.
KmsKeyId	No	Si decide cifrar el clúster, no podrá cambiar la AWS KMS clave que utilizó para cifrarlo.
MasterUsername	No	Una vez creado un clúster, no puede modificar el `MasterUsername` . Restricciones en la nomenclatura: • La longitud es de [1-63] caracteres alfanumér icos. • El primer carácter debe ser una letra. • No puede ser una palabra reservada por el motor de base de datos.

MasterUserPassword	Sí	Restricciones:
		
		• La longitud es de 8 a 100 caracteres ASCII imprimibles.
		• Se puede utilizar cualquier carácter ASCII imprimible, excepto los siguientes:
		  • **/** (barra inclinada)
		  • **"** (comillas dobles)
		  • **@** (símbolo de arroba)

Port	Sí	El número de puerto se aplica a todas las instancias del clúster.

Parámetro	Modificable	Notas
PreferredBackupWindow	Sí	
PreferredMaintenanceWindow	Sí	
StorageEncrypted	No	Si elige cifrar el clúster, no se puede descifrar.
StorageType	Sí	Tipo de almacenamiento para el clúster de DB: estándar (`standard`) u optimizado para E/S (`iopt1`). Valor predeterminado: `standard` Este parámetro se puede configurar con `CreateDBCluster` y. `ModifyDBCluster` Para obtener más información, consulte Configuraciones de almacenamiento en clústeres de Amazon DocumentDB.
Tags	Sí	
VpcSecurityGroupIds	No	Una vez creado un clúster, no puede modificar la VPC en la que reside el clúster.

Configuraciones de almacenamiento en clústeres de Amazon DocumentDB

A partir de Amazon DocumentDB 5.0, los clústeres basados en instancias admiten dos tipos de configuraciones de almacenamiento:

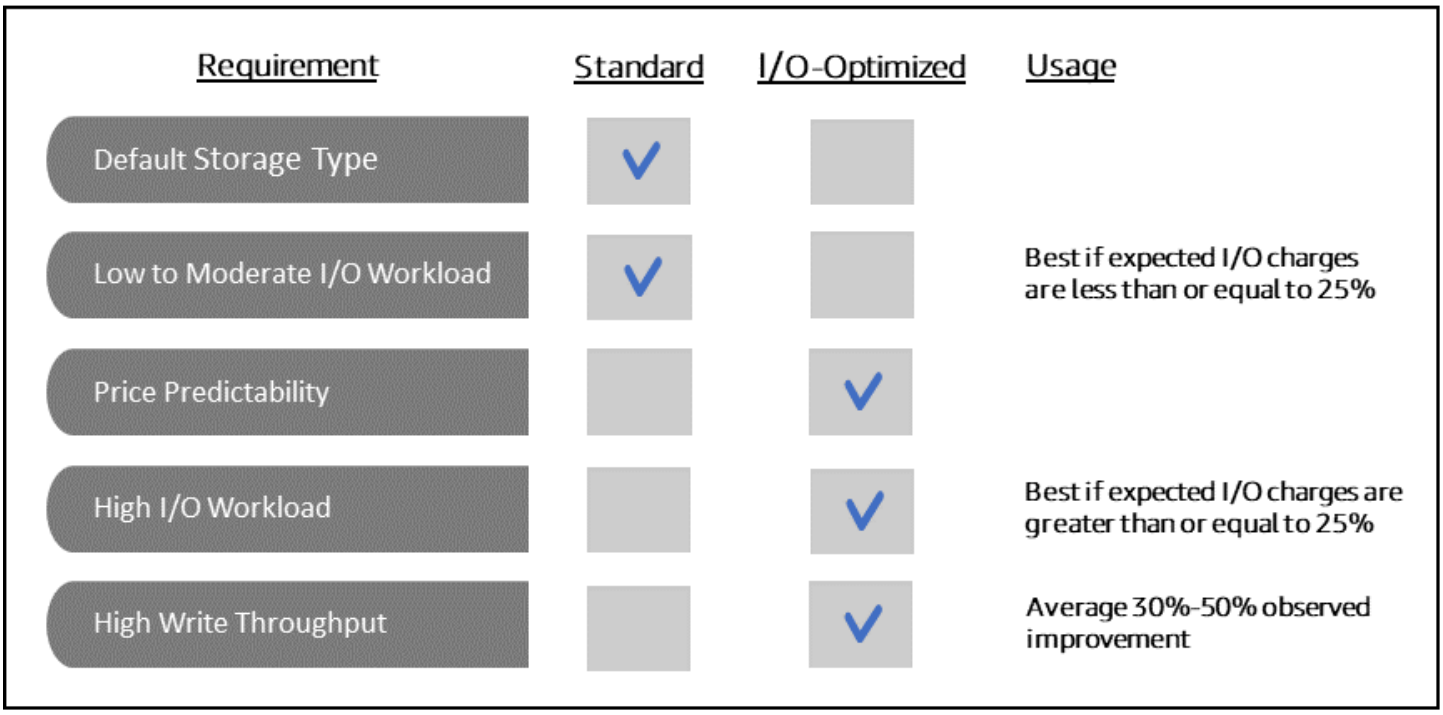
- Almacenamiento estándar de Amazon DocumentDB: diseñado para clientes con un consumo bajo a moderado I/O . Si espera que sus I/O costes sean inferiores al 25% del total de su clúster de Amazon DocumentDB, esta opción puede ser ideal para usted. Con la configuración de almacenamiento estándar de Amazon DocumentDB, se le facturará de pay-per-request I/O forma independiente a los cargos de instancia y almacenamiento. Esto significa que su facturación puede

variar de un ciclo a otro en función del uso. La configuración está diseñada para adaptarse a las I/O demandas fluctuantes de su aplicación.

- Almacenamiento optimizado para E/S de Amazon DocumentDB: diseñado para clientes que priorizan la previsibilidad de los precios o que tienen aplicaciones intensivas. I/O Las I/O-optimized configuration offers improved performance, increased throughput, and reduced latency for customers with I/O intensive workloads. If you expect your I/O costs to exceed 25% of your total Amazon DocumentDB cluster costs, this option offers enhanced price performance. With the Amazon DocumentDB I/O-optimized storage configuration, you won't be charged based on I/O operaciones, que garantizan costos predecibles en cada ciclo de facturación. La configuración estabiliza los costos y, al mismo tiempo, mejora el rendimiento.

Puede cambiar los clústeres de bases de datos existentes una vez cada 30 días a Amazon DocumentDB: I/O-optimized storage. You can switch back to Amazon DocumentDB standard storage at any time. The next date to modify the storage configuration to I/O optimizados y se puede realizar un seguimiento con el `describe-db-clusters` comando mediante la página de configuración del Consola de administración de AWS clúster AWS CLI o a través de ella.

Puede crear un nuevo clúster de bases de datos que incluya la configuración optimizada para E/S de Amazon DocumentDB o convertir los clústeres de bases de datos existentes con unos pocos clics en el Consola de administración de AWS, un solo cambio de parámetro en AWS Command Line Interface (AWS CLI) o mediante. AWS SDKs No es necesario interrumpir ni reiniciar las instancias durante o después de modificar la configuración de almacenamiento.

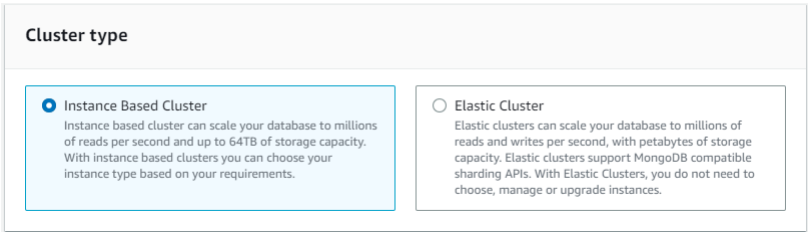


Creación de un clúster con optimización de E/S

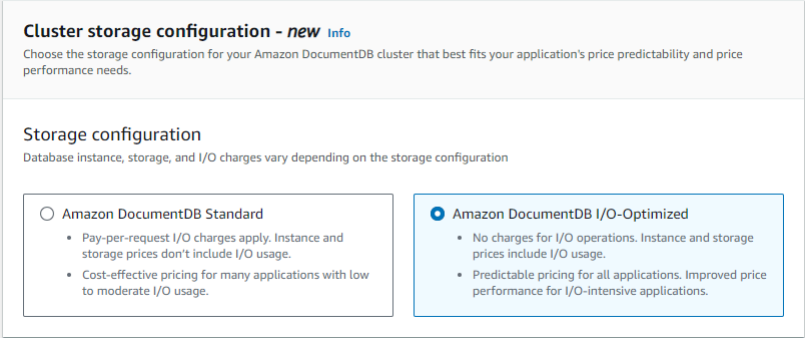
Using the Consola de administración de AWS

Cómo crear o modificar un clúster optimizado para E/S mediante la Consola de administración de AWS:

1. En la consola de administración de Amazon DocumentDB, en Clústeres, elija Crear o seleccione el clúster, elija Acciones y, a continuación, elija Modificar.
2. Si va a crear un clúster nuevo, asegúrese de elegir Clúster basado en instancias en la sección Tipo de clúster (esta es la opción predeterminada).



3. En la sección Configuración, en Configuración del almacenamiento en clúster, elija Amazon DocumentDB optimizado para E/S.



4. Complete la creación o modificación del clúster y elija Crear clúster o Modificar clúster.

   Para ver el proceso completo de creación de un clúster, consulte Crear un clúster y una instancia principal mediante Consola de administración de AWS.

   Para ver el proceso completo de modificación de un clúster, consulte Modificación de un clúster de Amazon DocumentDB.

Using the AWS CLI

Cómo crear un clúster optimizado para E/S mediante la AWS CLI:

En los siguientes ejemplos, sustituya cada uno por su *user input placeholder* propia información.

Para Linux, macOS o Unix:

```
aws docdb create-db-cluster \
      --db-cluster-identifier sample-cluster \
      --engine docdb \
      --engine-version 5.0.0 \
      --storage-type iopt1 \
      --deletion-protection \
      --master-username username \
      --master-user-password password
```

Para Windows:

```
aws docdb create-db-cluster ^
      --db-cluster-identifier sample-cluster ^
      --engine docdb ^
      --engine-version 5.0.0 ^
      --storage-type iopt1 ^
```

```
    --deletion-protection ^
    --master-username username ^
    --master-user-password password
```

Análisis de costos para determinar la configuración del almacenamiento

Con Amazon DocumentDB, tiene la flexibilidad de elegir la configuración de almacenamiento para cada clúster de bases de datos que tenga. Para asignar correctamente sus clústeres entre la opción estándar y optimizada para E/S, puede hacer un seguimiento de los costos de Amazon DocumentDB por clústeres. Para ello, puede agregar etiquetas a los clústeres existentes, habilitar el etiquetado de asignación de costos en el panel de Administración de facturación y costos de AWS y analizar los costos de un clúster determinado en el AWS Cost Explorer Service. Para obtener información sobre el análisis de costos, consulte nuestro blog Using cost allocation tags.

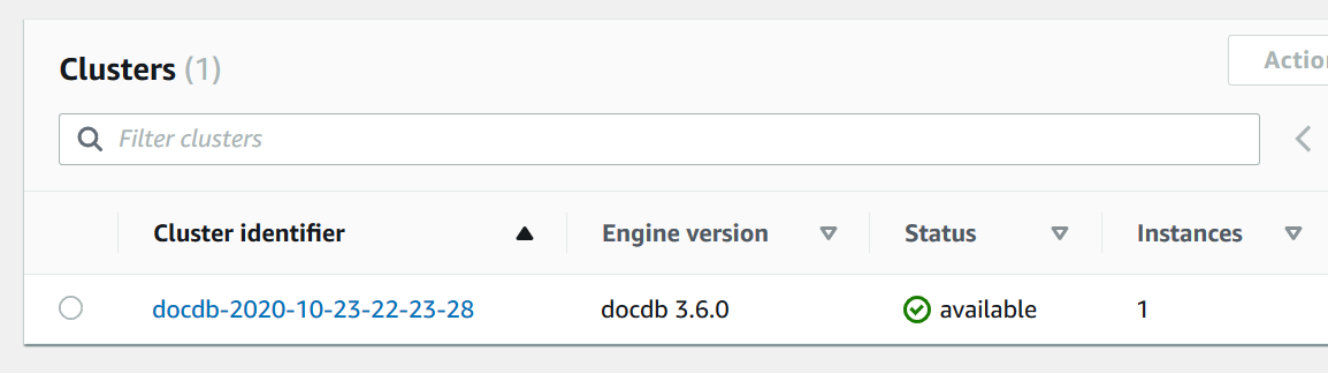
Determinación del estado de un clúster

Para determinar el estado de un clúster, utilice la tecla Consola de administración de AWS o AWS CLI.

Using the Consola de administración de AWS

Utilice el siguiente procedimiento para ver el estado del clúster de Amazon DocumentDB mediante el Consola de administración de AWS

1. Inicie sesión en y abra la Consola de administración de AWS consola de Amazon DocumentDB en https://console.aws.amazon.com /docdb.
2. En el panel de navegación, seleccione Clusters (Clústeres).
3. En la columna Cluster identifier (Identificador de clúster), busque el nombre del clúster que le interese. A continuación, para encontrar el estado del clúster, consulte en esa fila la columna Status (Estado), tal y como se muestra a continuación.



Using the AWS CLI

Utilice la operación `describe-db-clusters` para ver el estado del clúster de Amazon DocumentDB mediante la AWS CLI.

El siguiente código busca el estado del clúster `sample-cluster`.

Para Linux, macOS o Unix:

```
aws docdb describe-db-clusters \
    --db-cluster-identifier sample-cluster  \
    --query 'DBClusters[*].[DBClusterIdentifier,Status]'
```

Para Windows:

```
aws docdb describe-db-clusters ^
    --db-cluster-identifier sample-cluster  ^
    --query 'DBClusters[*].[DBClusterIdentifier,Status]'
```

La salida de esta operación será similar a lo que se indica a continuación (formato JSON).

```
[
    [
        "sample-cluster",
        "available"
    ]
]
```

Ciclo de vida del clúster de Amazon DocumentDB

El ciclo de vida de un clúster de Amazon DocumentDB incluye crear, describir, modificar y eliminar el clúster. En esta sección se proporciona información sobre cómo realizar estos procesos.

Temas

- Creación de un clúster de Amazon DocumentDB
- Descripción de los clústeres de Amazon DocumentDB
- Modificación de un clúster de Amazon DocumentDB
- Determinación de las tareas de mantenimiento pendientes

- Actualización de un parche a la versión del motor de un clúster
- Detención e inicio de un clúster de bases de datos de Amazon DocumentDB
- Eliminación de un clúster de Amazon DocumentDB

Creación de un clúster de Amazon DocumentDB

Un clúster de Amazon DocumentDB consta de instancias y de un volumen de clúster que representa los datos del clúster. El volumen de clúster se replica de seis formas en tres zonas de disponibilidad como un único volumen virtual. El clúster contiene una instancia principal y, opcionalmente, hasta 15 instancias de réplica.

En las siguientes secciones se muestra cómo crear un clúster de Amazon DocumentDB utilizando el Consola de administración de AWS o el. AWS CLI A continuación, puede añadir instancias de réplica al clúster. Si utiliza la consola para crear el clúster de Amazon DocumentDB, se crea automáticamente una instancia principal al mismo tiempo. Si lo usa AWS CLI para crear su clúster de Amazon DocumentDB, una vez que el estado del clúster esté disponible, debe crear la instancia principal para ese clúster.

Requisitos previos

A continuación, se describen los requisitos previos para crear un clúster de Amazon DocumentDB.

Si no tiene uno Cuenta de AWS, complete los siguientes pasos para crear uno.

Para suscribirte a una Cuenta de AWS

1. Abrir https://portal.aws.amazon.com/billing/registro.
2. Siga las instrucciones que se le indiquen.

   Parte del procedimiento de registro consiste en recibir una llamada telefónica o mensaje de texto e indicar un código de verificación en el teclado del teléfono.

   Cuando te registras en un Cuenta de AWS, Usuario raíz de la cuenta de AWSse crea un. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario y utilice únicamente el usuario raíz para realizar tareas que requieren acceso de usuario raíz.

Requisitos previos de VPC

Solo puede crear un clúster de Amazon DocumentDB en una instancia de Amazon Virtual Private Cloud (Amazon VPC). Amazon VPC debe tener como mínimo una subred en al menos dos de las zonas de disponibilidad para que la use con un clúster de base de datos de Amazon DocumentDB. Mediante la distribución de las instancias del clúster en las zonas de disponibilidad, se garantiza que habrá instancias disponibles en el clúster en el caso improbable de que se produzca un error en una zona.

Requisitos previos de la subred

Al crear un clúster de Amazon DocumentDB, debe elegir una VPC y el grupo de subredes correspondiente dentro de la VPC para lanzar el clúster. Las subredes determinan la zona de disponibilidad y el rango de direcciones IP de esa zona de disponibilidad que se quieran utilizar para lanzar una instancia. Para los fines de esta exposición, usaremos los términos subred y zona de disponibilidad indistintamente. Un grupo de subredes es un conjunto de subredes (o zonas de disponibilidad). Un grupo de subredes le permite especificar las zonas de disponibilidad que desea utilizar para lanzar instancias de Amazon DocumentDB. Por ejemplo, para ofrecer un alto nivel de disponibilidad en un clúster con tres instancias, se recomienda que cada una de dichas instancias esté aprovisionada en una zona de disponibilidad distinta. De esa forma, si una de las zonas de disponibilidad deja de funcionar, solo se verá afectada una sola instancia.

Las instancias de Amazon DocumentDB actualmente pueden aprovisionarse en hasta tres zonas de disponibilidad. Aunque un grupo de subredes tenga más de tres subredes, solo podrá utilizar tres de esas subredes para crear un clúster de Amazon DocumentDB. Por ello, es aconsejable que al crear un grupo de subredes solo elija las tres subredes en las que desee implementar las instancias. En el este de EE. UU. (Norte de Virginia), el grupo de subredes puede tener seis subredes (o zonas de disponibilidad). Sin embargo, cuando se aprovisione un clúster de Amazon DocumentDB, Amazon DocumentDB elige tres de estas zonas de disponibilidad que utiliza para aprovisionar instancias.

Por ejemplo, supongamos que al crear un clúster, Amazon DocumentDB elige las zonas de disponibilidad {1A, 1B y 1C}. Si intenta crear una instancia en la zona de disponibilidad {1D}, la llamada a la API no funcionará correctamente. Sin embargo, si decide crear una instancia sin especificar la zona de disponibilidad concreta, Amazon DocumentDB elegirá una zona de disponibilidad por usted. Amazon DocumentDB utiliza un algoritmo para equilibrar la carga de las instancias en las zonas de disponibilidad para ayudarle a obtener una alta disponibilidad. Por ejemplo, si se aprovisionan tres instancias, de forma predeterminada se repartirán entre tres zonas de disponibilidad en lugar de aprovisionar todas ellas en una única zona de disponibilidad.

Recomendaciones:

- A menos que tenga un motivo específico, cree siempre un grupo de subredes con tres subredes. De esta forma, se asegurará de que los clústeres con tres o más instancias puedan lograr una mayor disponibilidad, debido a que las instancias se aprovisionarán en tres zonas de disponibilidad distintas.
- Reparta siempre las instancias en varias zonas de disponibilidad para lograr una alta disponibilidad. Nunca ponga todas las instancias de un clúster en una única zona de disponibilidad.
- Debido a que pueden producirse eventos de conmutación por error en cualquier momento, no debe dar por hecho que una instancia principal o las instancias de réplica siempre están en una zona de disponibilidad determinada.

Requisitos previos adicionales

A continuación se indican algunos requisitos adicionales para crear un clúster de Amazon DocumentDB:

- Si se conecta para AWS utilizar credenciales AWS Identity and Access Management (IAM), su cuenta de IAM debe tener políticas de IAM que concedan los permisos necesarios para realizar las operaciones de Amazon DocumentDB.

  Si utiliza una cuenta de IAM para acceder a la consola de Amazon DocumentDB, primero debe iniciar sesión en ella con su cuenta Consola de administración de AWS de IAM. A continuación, vaya a la consola de Amazon DocumentDB en https://console.aws.amazon.com /docdb.
- Si desea adaptar los parámetros de configuración a un clúster, debe especificar un grupo de parámetros de clúster y un grupo de parámetros con la configuración de parámetros necesaria. Para obtener información acerca de cómo crear o modificar un grupo de parámetros de clúster o un grupo de parámetros de base de datos, consulte Administración de los grupos de parámetros de clúster de Amazon DocumentDB.
- Debe determinar el número de TCP/IP puerto que desea especificar para el clúster. Los firewalls de algunas compañías bloquean las conexiones a estos puertos predeterminados para Amazon DocumentDB. Si el firewall de su compañía bloquea el puerto predeterminado, elija otro puerto para el clúster. Todas las instancias de un clúster usan el mismo puerto.

Crear un clúster y una instancia principal mediante Consola de administración de AWS

Los siguientes procedimientos describen cómo se usa la consola para lanzar un clúster de Amazon DocumentDB con una o varias instancias.

Creación de un clúster: uso de la configuración predeterminada

Para crear un clúster con instancias que utilicen la configuración predeterminada, utilice la Consola de administración de AWS

1. Inicie sesión en y abra la Consola de administración de AWS consola de Amazon DocumentDB en https://console.aws.amazon.com /docdb.
2. Si desea crear su clúster en una región que no Región de AWS sea EE. UU. Este (Virginia del Norte), elija la región de la lista que aparece en la sección superior derecha de la consola.
3. En el panel de navegación, elija Clusters (Clústeres) y, a continuación, elija Create (Crear).

   > **Tip**
   >
   > Si no ve el panel de navegación del lado izquierdo de la pantalla, seleccione el icono de menú
   > (≡)
   > en la esquina superior izquierda de la página.

4. En la página Crear clúster de Amazon DocumentDB, complete el panel de Configuración.

   a. Identificador de clúster: acepte el nombre que ha proporcionado Amazon DocumentDB o introduzca un nombre para el clúster; por ejemplo, **`sample-cluster`**.

      Restricciones en cuanto a la nomenclatura de los clústeres:

      - Debe tener [1-63] letras, números o guiones.
      - El primer carácter debe ser una letra.
      - No puede terminar con un guion ni contener dos guiones consecutivos.
      - Debe ser único para todos los clústeres de Amazon RDS, Neptune y Amazon DocumentDB por región. Cuenta de AWS

   b. Versión del motor: acepte la versión del motor predeterminada (5.0.0), o, si lo desea, elija la 4.0.0 o 3.6.0.

c. Clase de instancia: puede aceptar la `db.r5.large` predeterminada o elegir una en la lista desplegable.

d. Número de instancias: en la lista, elija el número de instancias que desee crear cuando se restaure el clúster. La primera es la instancia principal, todas las demás instancias son instancias de réplica de solo lectura. Puede añadir y eliminar instancias más adelante si las necesita. De forma predeterminada, un clúster de Amazon DocumentDB se lanzará con tres instancias (una principal y dos réplicas).

5. Complete la sección Configuración del almacenamiento en clúster.

   Elija Amazon DocumentDB estándar (predeterminado) o Amazon DocumentDB optimizado para E/S. Para obtener más información, consulte Configuraciones de almacenamiento en clústeres de Amazon DocumentDB.

6. Rellene el panel Authentication (Autenticación).

   a. Nombre de usuario: ingrese un nombre para el usuario principal. Para iniciar sesión en el clúster, debe utilizar el nombre de usuario principal.

      Restricciones de denominación de usuario principal:

      - La longitud es de [1-63] caracteres alfanuméricos.
      - El primer carácter debe ser una letra.
      - No puede ser una palabra reservada por el motor de base de datos.

   b. Seleccione una de las siguientes opciones de contraseña:

      - Administrado en AWS Secrets Manager: elija esta opción si desea administrar automáticamente la contraseña AWS Secrets Manager de su usuario principal.

        Si elige esta opción, configure la clave KMS. Para ello, cree la suya propia o utilice una clave creada por Secrets Manager.

      - Autoadministrado: elija esta opción si desea autoadministrar la contraseña de su usuario principal. Si elige esta opción, introduzca una contraseña para el usuario principal y confírmela. Para iniciar sesión en el clúster, debe utilizar la contraseña del usuario principal.

        Restricciones para la contraseña:

        - La longitud es de [8-100] caracteres ASCII imprimibles.
        - Se puede utilizar cualquier carácter ASCII imprimible, excepto los siguientes:

- **/** (barra inclinada)
- **"** (comillas dobles)
- **@** (símbolo de arroba)

7. En la parte inferior de la pantalla, elija una de las opciones siguientes:
   - Para crear el clúster ahora, elija Create cluster (Crear clúster).
   - Si no desea crear el clúster, elija Cancel (Cancelar).
   - Para configurar el clúster antes de crearlo, elija Show additional configurations (Mostrar configuraciones adicionales) y, a continuación, continúe en Creación de un clúster: configuraciones adicionales.

     Las configuraciones que aparecen en Additional Configurations (Configuraciones adicionales) son las siguientes:

     - Configuración de red: el valor predeterminado es utilizar el grupo de seguridad de VPC `default`.
     - Opciones de clúster: de forma predeterminada, se utilizan el puerto 27017 y el grupo de parámetros predeterminado.
     - Cifrado: el valor predeterminado es habilitar el cifrado con la clave `(default) aws/rds`.

       > **Important**
       >
       > Después de que se cifra un clúster, no es posible descifrarlo.

     - Copia de seguridad: el valor predeterminado es conservar las copias de seguridad durante 1 día y dejar que Amazon DocumentDB seleccione el periodo de copia de seguridad.
     - Exportaciones de registros: el valor predeterminado es no exportar los registros de auditoría a los CloudWatch registros.
     - Mantenimiento: de forma predeterminada, Amazon DocumentDB elige el período de mantenimiento.
     - Protección contra la eliminación: proteja sus clústeres contra la eliminación accidental. El valor predeterminado para el clúster creado con la consola es enabled (habilitado).

Si acepta los valores predeterminados ahora, podrá cambiar la mayoría de ellos más adelante modificando el clúster.

8. Habilite la conexión entrante del grupo de seguridad de su clúster.

   Si no ha cambiado la configuración predeterminada de su clúster, ha creado un clúster mediante el grupo de seguridad predeterminado para la VPC predeterminada en una región en concreto. Para conectarse a Amazon DocumentDB, tiene que habilitar las conexiones entrantes en el puerto 27017 (o el puerto que prefiera) para el grupo de seguridad de su clúster.

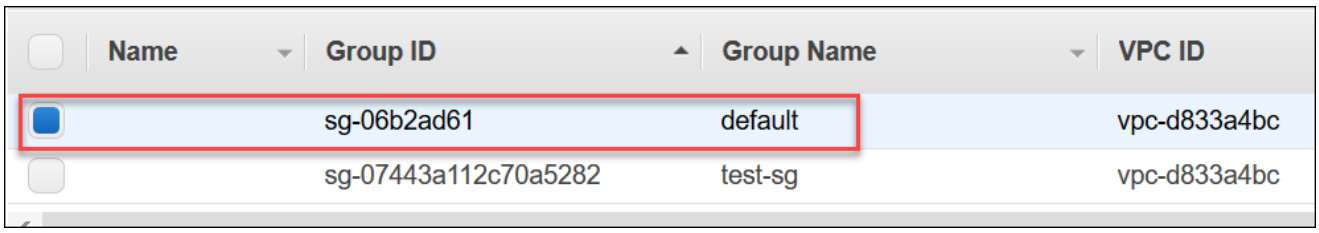
   Cómo añadir una conexión entrante al grupo de seguridad de su clúster

   a. Inicia sesión en la EC2 consola de Amazon Consola de administración de AWS y ábrela en https://console.aws.amazon.com/ec2/.

   b. En la sección Resources (Recursos) de la ventana principal, seleccione Security groups (Grupos de seguridad).



   c. En la lista de grupos de seguridad, localice el grupo de seguridad que utilizó para crear el clúster (lo más probable es que fuera el grupo de seguridad predeterminado) y seleccione la casilla situada a la izquierda del nombre del grupo de seguridad.



   d. En el menú Actions (Acciones), elija Edit inbound rules (Editar reglas entrantes) y, a continuación, seleccione o especifica las restricciones de las reglas.

      i. Tipo: en la lista, elija el protocolo para abrir al tráfico de la red.

ii. Protocolo: en la lista, elija el tipo de protocolo.

iii. Intervalo de puertos: para una regla personalizada, introduzca un número de puerto o un intervalo de puertos. Asegúrese de que el número de puerto o el rango de puertos incluye el puerto que especificó cuando creó el clúster (predeterminado: 27017).

iv. Origen: especifica el tráfico que puede llegar a su instancia. En la lista, elija el origen del tráfico. Si selecciona Custom (Personalizado), especifique una única dirección IP o un rango de direcciones IP en notación CIDR (p. ej., 203.0.113.5/32).

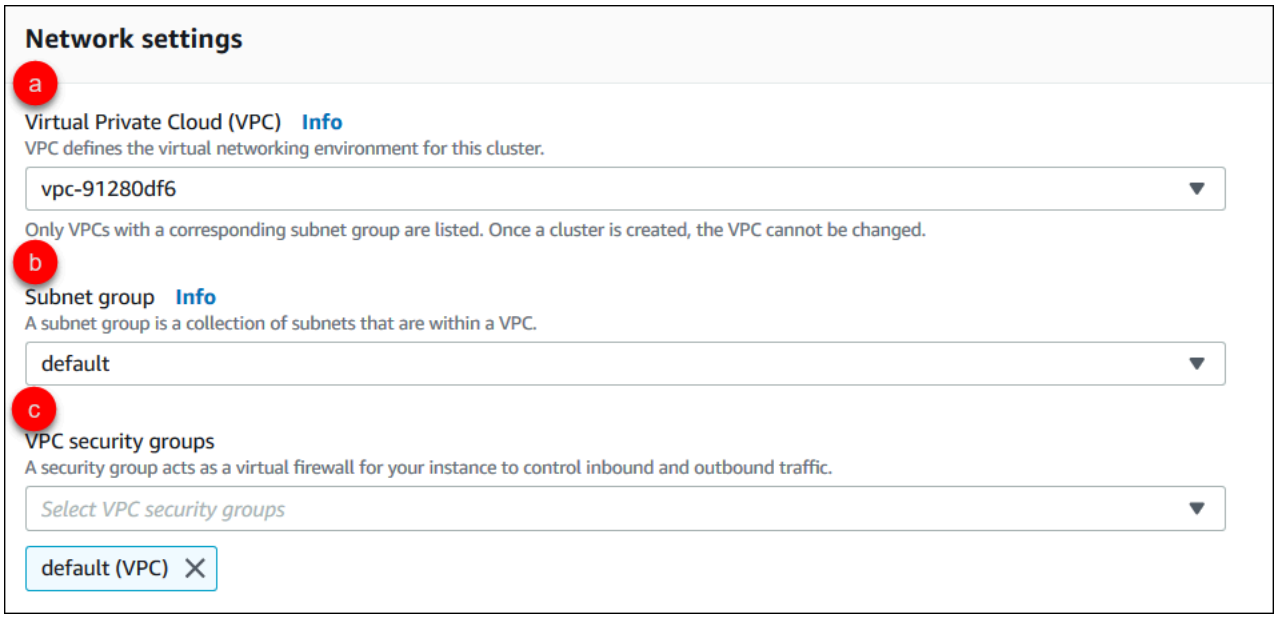
v. Descripción: escriba una descripción para la regla.

vi. Cuando finalice la creación de la regla, seleccione Save (Guardar).

Creación de un clúster: configuraciones adicionales

Si desea aceptar los valores predeterminados para el clúster, puede omitir los pasos que se describen a continuación y elegir Create cluster (Crear clúster).

1. Rellene el panel Network settings (Configuración de red).



a. Nube privada virtual (VPC): en la lista, elija la Amazon VPC en la que desea lanzar este clúster.

b. Grupo de subredes: en la lista, elija el grupo de subredes que desea utilizar para este clúster.

c. Grupos de seguridad de VPC: en la lista, elija el grupo de seguridad para el clúster.

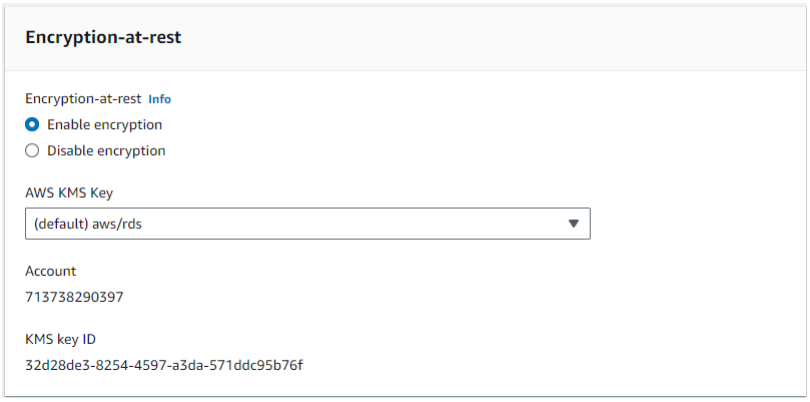
2. Rellene el panel Cluster options (Opciones de clúster).



   a. Puerto de base de datos: usa las flechas arriba y abajo para configurar el TCP/IP puerto que usarán las aplicaciones para conectarse a tu instancia.

   b. Grupo de parámetros de clúster: en la lista de grupos de parámetros, elija el grupo de parámetros de clúster para este clúster.

3. Rellene el panel Encryption (Cifrado).



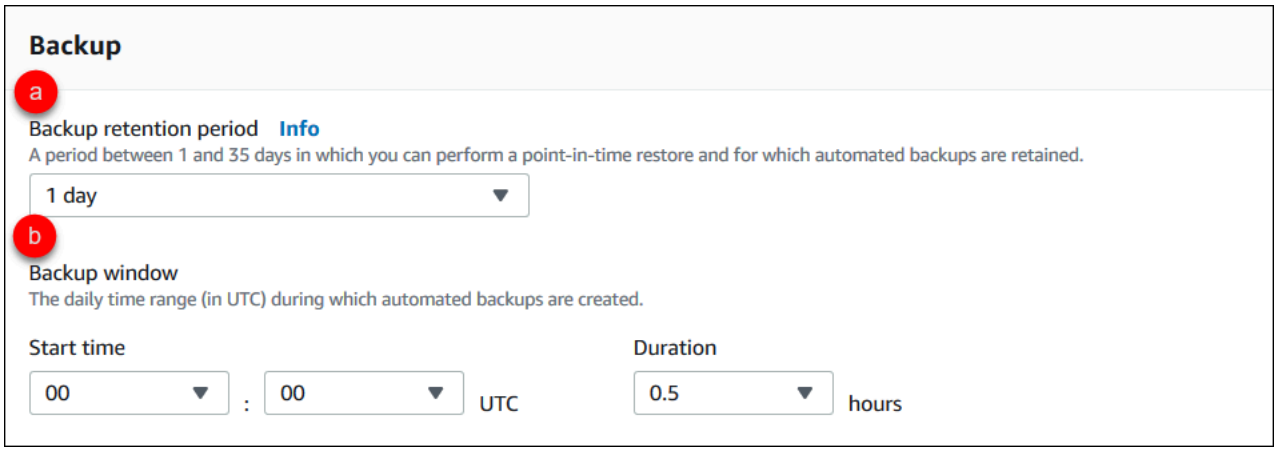
   a. E ncryption-at-rest: elija una de las siguientes opciones:

      - Habilitar el cifrado: de manera predeterminada. Se cifran todos los datos en reposo. Si decide cifrar los datos, no puede deshacer esta acción.
      - Deshabilitar cifrado: los datos no se cifran.

   b. AWS Clave KMS: solo está disponible si está cifrando sus datos. En la lista, elija la clave que desee utilizar para cifrar los datos de este clúster. El valor predeterminado es `(default) aws/rds`.

      Si ha elegido, Enter a key ARN (Escribir un ARN de clave), tendrá que introducir un nombre de recurso de Amazon (ARN) para la clave.

4. Rellene el panel Backup (Copia de seguridad).



   a. Periodo de retención de copias de seguridad: en la lista, elija el número de días que se deben conservar las copias de seguridad automáticas de este clúster antes de eliminarlas.

   b. Periodo de copia de seguridad: especifique la hora del día en que Amazon DocumentDB debe hacer las copias de seguridad de este clúster y la duración de las mismas.

      i. Hora de inicio: en la primera lista, elija la hora de inicio (UTC) para las copias de seguridad automáticas. En la segunda lista, elija el minuto de la hora en que desea que comiencen las copias de seguridad automáticas.

      ii. Duración: en la lista, elija el número de horas que se deben asignar para crear las copias de seguridad automáticas.

5. Complete el panel de exportaciones de registros seleccionando los tipos de registros que desea exportar a CloudWatch Logs.

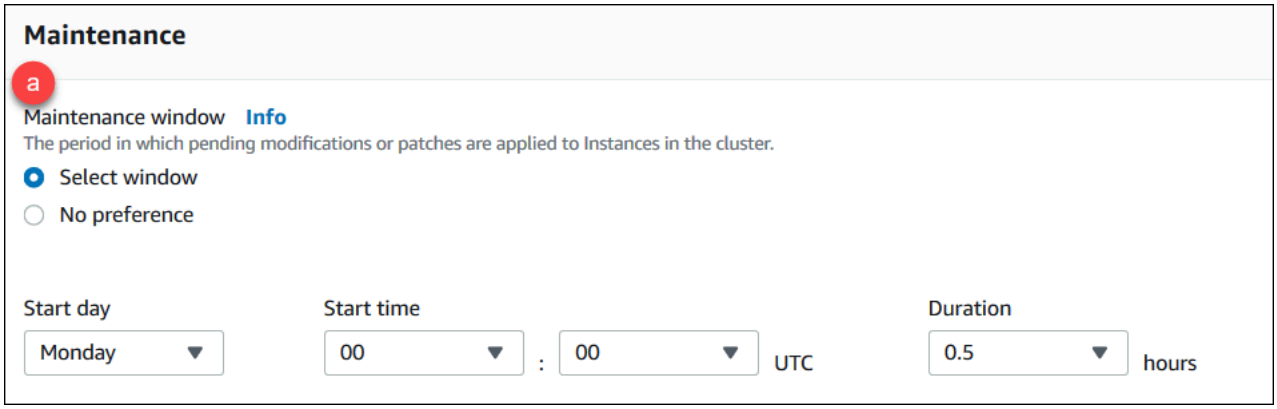


   - Registros de auditoría: seleccione esta opción para permitir la exportación de registros de auditoría a Amazon CloudWatch Logs. Si selecciona Audit logs (Registros de auditoría), debe habilitar `audit_logs` en el grupo de parámetros personalizado del clúster. Para obtener más información, consulte Auditoría de eventos de Amazon DocumentDB.
   - Registros del generador de perfiles: seleccione esta opción para permitir la exportación de los registros del generador de perfiles de operaciones a Amazon Logs. CloudWatch Si selecciona Profiler logs (Registros del generador de perfiles), también debe modificar los siguientes parámetros en el grupo de parámetros personalizado del clúster:

- `profiler` establezca en `enabled`.
- `profiler_threshold_ms` establezca en un valor `[0-INT_MAX]` para definir el umbral para las operaciones de creación de perfiles.
- `profiler_sampling_rate` establezca en un valor `[0.0-1.0]` para establecer el porcentaje de operaciones lentas en el perfil.

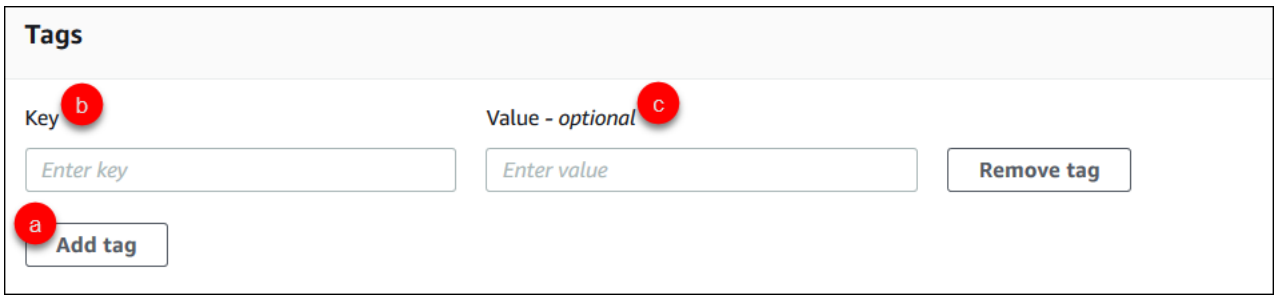
Para obtener más información, consulte Creación de perfiles de operaciones en Amazon DocumentDB.

6. Rellene el panel Maintenance (Mantenimiento).



- Elija una de las opciones siguientes.
  - Seleccionar periodo: permite especificar el día de la semana y la hora de inicio UTC en que Amazon DocumentDB debe realizar el mantenimiento del clúster y la duración de esta operación.
    a. Día de inicio: en la lista, elija el día de la semana en que debe iniciarse el mantenimiento del clúster.
    b. Hora de inicio: en las listas, elija la hora UTC y el minuto UTC en que debe iniciarse el mantenimiento.
    c. Duración: en la lista, elija el tiempo que se debe asignar para mantenimiento del clúster. Si el mantenimiento no puede finalizar en el tiempo especificado, el proceso de mantenimiento continuará pasado ese tiempo hasta que finalice.
  - Sin preferencia: Amazon DocumentDB selecciona el día de la semana, la hora de inicio y la duración para realizar el mantenimiento.

7. Si desea añadir una o más etiquetas a este clúster, complete el panel Tags (Etiquetas).



Para cada etiqueta que desee añadir al clúster, repita los pasos siguientes. Puede disponer de hasta 10 en un clúster.

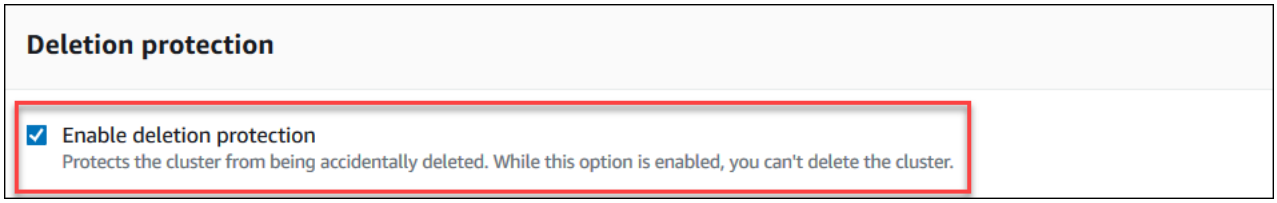
a. Elija Add tags (Añadir etiquetas).

b. Escriba la clave de la etiqueta.

c. Si lo desea, escriba el valor de la etiqueta.

Para quitar una etiqueta, elija Remove tag (Eliminar etiqueta).

8. La protección contra eliminación se habilita de forma predeterminada cuando crea un clúster mediante la consola. Para deshabilitar la protección contra eliminación, desactive Habilitar la protección contra eliminación. Cuando esté habilitada, la protección contra eliminación evitará que se elimine un clúster. Para quitar un clúster protegido contra eliminación, en primer lugar debe modificar el clúster para deshabilitar la protección contra eliminación.



Para obtener más información sobre la protección contra eliminación, consulte Eliminación de un clúster de Amazon DocumentDB.

9. Para crear el clúster, elija Create cluster (Crear clúster). De lo contrario, seleccione Cancelar.

Creación de un clúster mediante AWS CLI

Los siguientes procedimientos describen cómo utilizarlos AWS CLI para lanzar un clúster de Amazon DocumentDB y crear una réplica de Amazon DocumentDB.

Parameters

- **`--db-cluster-identifier`**: obligatorio. Una cadena en minúsculas que identifica este clúster.

  Restricciones en cuanto a la nomenclatura de los clústeres:

  - Debe tener [1-63] letras, números o guiones.
  - El primer carácter debe ser una letra.
  - No puede terminar con un guion ni contener dos guiones consecutivos.
  - Debe ser único para todos los clústeres (en Amazon RDS, Amazon Neptune y Amazon DocumentDB) AWS por cuenta y región.

- **`--engine`**: obligatorio. Debe ser **`docdb`**.
- **`--deletion-protection | --no-deletion-protection`**: opcional. Cuando la protección contra eliminación esté habilitada, evitará que se elimine un clúster. Cuando se utiliza AWS CLI, la configuración predeterminada es desactivar la protección contra la eliminación.

  Para obtener más información sobre la protección contra eliminación, consulte Eliminación de un clúster de Amazon DocumentDB.
- **`--storage-type standard | iopt1`**: opcional. Predeterminado: **`standard`**. Configuración de almacenamiento en clústeres. Los valores válidos son `standard` (estándar) o `iopt1` (optimizado para E/S).
- **`--master-username`**: obligatorio. El nombre de usuario que se utiliza para autenticar al usuario.

  Restricciones en cuanto a la nomenclatura de los usuarios maestros:

  - La longitud es de [1-63] caracteres alfanuméricos.
  - El primer carácter debe ser una letra.
  - No puede ser una palabra reservada por el motor de base de datos.

- **`--master-user-password`**: opcional. La contraseña de usuario que se utiliza para autenticar al usuario.

  Restricciones para la contraseña maestra:

  - La longitud es de [8-100] caracteres ASCII imprimibles.

  - Se puede utilizar cualquier carácter ASCII imprimible, excepto los siguientes:
    - **/** (barra inclinada)
    - **"** (comillas dobles)
    - **@** (símbolo de arroba)

- **`--manage-master-user-password`**: opcional. Amazon DocumentDB genera la contraseña del usuario maestro y la administra durante todo su ciclo de vida en Secrets Manager.

Para ver otros parámetros, consulte CreateDBCluster.

Para lanzar un clúster de Amazon DocumentDB mediante AWS CLI

Para crear un clúster de Amazon DocumentDB, llame a. `create-db-cluster` AWS CLI El siguiente AWS CLI comando crea un clúster de Amazon DocumentDB denominado `sample-cluster` con la protección de eliminación habilitada. Para obtener más información sobre la protección contra eliminación, consulte Eliminación de un clúster de Amazon DocumentDB.

Además, `--engine-version` es un parámetro opcional que utiliza de forma predeterminada la última versión principal del motor. La versión actual del motor principal es la 5.0.0. Cuando se publiquen nuevas versiones principales del motor, la versión del motor predeterminada para `--engine-version` se actualizará para reflejar la última versión principal del motor. Por lo tanto, para las cargas de trabajo de producción, y especialmente las que dependen de la creación de scripts, la automatización o CloudFormation las plantillas, le recomendamos que especifique explícitamente la versión `--engine-version` principal prevista.

> **Note**
>
> Si no se especifica un `db-subnet-group-name` o un `vpc-security-group-id`, Amazon DocumentDB utilizará el grupo de subredes y el grupo de seguridad de Amazon VPC predeterminados para la región determinada.

Para Linux, macOS o Unix:

```
aws docdb create-db-cluster \
      --db-cluster-identifier sample-cluster \
      --engine docdb \
      --engine-version 5.0.0 \
```

```
      --deletion-protection \
      --master-username masteruser \
      --master-user-password password
```

Para Windows:

```
aws docdb create-db-cluster ^
      --db-cluster-identifier sample-cluster ^
      --engine docdb ^
      --engine-version 5.0.0 ^
      --deletion-protection ^
      --master-username masteruser ^
      --master-user-password password
```

La salida de esta operación será similar a lo que se indica a continuación (formato JSON).

```
{
    "DBCluster": {
        "StorageEncrypted": false,
        "DBClusterMembers": [],
        "Engine": "docdb",
        "DeletionProtection" : "enabled",
        "ClusterCreateTime": "2018-11-26T17:15:19.885Z",
        "DBSubnetGroup": "default",
        "EngineVersion": "5.0.0",
        "MasterUsername": "masteruser",
        "BackupRetentionPeriod": 1,
        "DBClusterArn": "arn:aws:rds:us-east-1:123456789012:cluster:sample-cluster",
        "DBClusterIdentifier": "sample-cluster",
        "MultiAZ": false,
        "DBClusterParameterGroup": "default.docdb5.0",
        "PreferredBackupWindow": "09:12-09:42",
        "DbClusterResourceId": "cluster-KQSGI4MHU4NTDDRVNLNTU7XVAY",
        "PreferredMaintenanceWindow": "tue:04:17-tue:04:47",
        "Port": 27017,
        "Status": "creating",
        "ReaderEndpoint": "sample-cluster.cluster-ro-sfcrlcjcoroz.us-
east-1.docdb.amazonaws.com",
        "AssociatedRoles": [],
        "HostedZoneId": "ZNKXTT8WH85VW",
        "VpcSecurityGroups": [
            {
                "VpcSecurityGroupId": "sg-77186e0d",
```

```
                "Status": "active"
            }
        ],
        "AvailabilityZones": [
            "us-east-1a",
            "us-east-1c",
            "us-east-1e"
        ],
        "Endpoint": "sample-cluster.cluster-sfcrlcjcoroz.us-east-1.docdb.amazonaws.com"
    }
}
```

La creación del clúster puede tardar varios minutos. Puede utilizar la Consola de administración de AWS o AWS CLI para supervisar el estado de su clúster. Para obtener más información, consulte Supervisión del estado de un clúster de Amazon DocumentDB.

> **Important**
>
> Cuando se utiliza AWS CLI para crear un clúster de Amazon DocumentDB, no se crea ninguna instancia. Por lo tanto, tendrá que crear de forma explícita una instancia principal y las instancias de réplica que necesite. Puede usar la consola o AWS CLI para crear las instancias. Para obtener más información, consulte Agregación de una instancia de Amazon DocumentDB a un clúster.

Para obtener más información, consulte `CreateDBCluster` en la Referencia de la API de Amazon DocumentDB.

Descripción de los clústeres de Amazon DocumentDB

Puede utilizar la consola de administración de Amazon DocumentDB o la AWS CLI para ver detalles como los puntos de conexión, los grupos de seguridad y los grupos de parámetros relacionados con sus clústeres de Amazon DocumentDB. VPCs

Para obtener más información, consulte los siguientes temas:

- Supervisión del estado de un clúster de Amazon DocumentDB
- Búsqueda de puntos de conexión de un clúster

Using the Consola de administración de AWS

Use el siguiente procedimiento para ver los detalles de un clúster de Amazon DocumentDB especificado mediante la consola.

1. Inicie sesión en y abra la Consola de administración de AWS consola de Amazon DocumentDB en https://console.aws.amazon.com /docdb.
2. En el panel de navegación, seleccione Clusters (Clústeres).

   > **Tip**
   >
   > Si no ve el panel de navegación del lado izquierdo de la pantalla, seleccione el icono de menú
   > (≡)
   > en la esquina superior izquierda de la página.

3. En la lista de clústeres, elija el nombre del clúster cuyos detalles desea ver. La información sobre el clúster está organizada en las siguientes agrupaciones:

   - Resumen: información general sobre el clúster, incluida la versión del motor, el estado del clúster, el mantenimiento pendiente y el estado de su grupo de parámetros.
   - Conectividad y seguridad: la sección Conectar muestra los puntos de conexión para conectarse a este clúster con el shell de mongo o con una aplicación. La sección Grupos de seguridad muestra los grupos de seguridad asociados a este clúster y su ID de VPC y descripciones.
   - Configuración la sección Detalles del clúster muestra detalles sobre el clúster, incluidos el nombre de recurso de Amazon (ARN), el punto de conexión y el grupo de parámetros de clúster. También muestra la información de copia de seguridad del clúster, los detalles de mantenimiento y la configuración de seguridad y red. La sección Instancias del clúster muestra las instancias que pertenecen a este clúster con el rol de cada instancia y el estado del grupo de parámetros del clúster.
   - Supervisión: las métricas de Amazon CloudWatch Logs de este clúster. Para obtener más información, consulte Supervisión de Amazon DocumentDB con CloudWatch.
   - Eventos y etiquetas: en la sección de eventos recientes se enumeran los eventos recientes de este clúster. Amazon DocumentDB mantiene un registro de los eventos relacionados con los clústeres, las instancias, las instantáneas, los grupos de seguridad y los grupos de

parámetros de clúster. Esta información incluye la fecha, la hora y el mensaje asociados a cada evento. La sección Etiquetas muestra las etiquetas asociadas a este clúster.

Using the AWS CLI

Para ver los detalles de sus clústeres de Amazon DocumentDB mediante el AWS CLI, utilice el `describe-db-clusters` comando tal y como se muestra en los ejemplos siguientes. Para obtener más información, consulte `DescribeDBClusters` en la Referencia de la API para administración de recursos de Amazon DocumentDB.

> **Note**
>
> Para ciertas características de administración, como la administración del ciclo de vida de clúster y de instancia, Amazon DocumentDB aprovecha la tecnología operativa que se comparte con Amazon RDS. El parámetro de filtro `filterName=engine,Values=docdb` devuelve solo clústeres de Amazon DocumentDB.

Example

Ejemplo 1: enumerar todos los clústeres de Amazon DocumentDB

El AWS CLI código siguiente muestra los detalles de todos los clústeres de Amazon DocumentDB de una región.

```
aws docdb describe-db-clusters --filter Name=engine,Values=docdb
```

La salida de esta operación será similar a lo que se indica a continuación.

```
{
    "DBClusters": [
        {
            "AvailabilityZones": [
                "us-east-1c",
                "us-east-1b",
                "us-east-1a"
            ],
            "BackupRetentionPeriod": 1,
            "DBClusterIdentifier": "sample-cluster-1",
```

```
            "DBClusterParameterGroup": "sample-parameter-group",
            "DBSubnetGroup": "default",
            "Status": "available",
            ...
        },
        {
            "AvailabilityZones": [
                "us-east-1c",
                "us-east-1b",
                "us-east-1a"
            ],
            "BackupRetentionPeriod": 1,
            "DBClusterIdentifier": "sample-cluster-2",
            "DBClusterParameterGroup": "sample-parameter-group",
            "DBSubnetGroup": "default",
            "Status": "available",
            ...
        },
        {
            "AvailabilityZones": [
                "us-east-1c",
                "us-east-1b",
                "us-east-1a"
            ],
            "BackupRetentionPeriod": 1,
            "DBClusterIdentifier": "sample-cluster-3",
            "DBClusterParameterGroup": "sample-parameter-group",
            "DBSubnetGroup": "default",
            "Status": "available",
            ...
        }
    ]
}
```

Example

Ejemplo 2: mostrar todos los detalles de un clúster de Amazon DocumentDB especificado

En el AWS CLI código siguiente se enumeran los detalles del clúster`sample-cluster`.

Para Linux, macOS o Unix:

```
aws docdb describe-db-clusters \
   --filter Name=engine,Values=docdb \
```

```
   --db-cluster-identifier sample-cluster
```

Para Windows:

```
aws docdb describe-db-clusters ^
   --filter Name=engine,Values=docdb ^
   --db-cluster-identifier sample-cluster
```

La salida de esta operación será similar a lo que se indica a continuación.

```
{
    "DBClusters": [
        {
            "AllocatedStorage": 1,
            "AvailabilityZones": [
                "us-east-1c",
                "us-east-1a",
                "us-east-1d"
            ],
            "BackupRetentionPeriod": 2,
            "DBClusterIdentifier": "sample-cluster",
            "DBClusterParameterGroup": "sample-parameter-group",
            "DBSubnetGroup": "default",
            "Status": "available",
            "EarliestRestorableTime": "2023-11-07T22:34:08.148000+00:00",
            "Endpoint": "sample-cluster.node.us-east-1.amazon.com",
            "ReaderEndpoint": "sample-cluster.node.us-east-1.amazon.com",
            "MultiAZ": false,
            "Engine": "docdb",
            "EngineVersion": "5.0.0",
            "LatestRestorableTime": "2023-11-10T07:21:16.772000+00:00",
            "Port": 27017,
            "MasterUsername": "chimeraAdmin",
            "PreferredBackupWindow": "22:22-22:52",
            "PreferredMaintenanceWindow": "sun:03:01-sun:03:31",
            "ReadReplicaIdentifiers": [],
            "DBClusterMembers": [
                {
                    "DBInstanceIdentifier": "sample-instance-1",
                    "IsClusterWriter": true,
                    "DBClusterParameterGroupStatus": "in-sync",
                    "PromotionTier": 1
                },
```

```
                {
                    "DBInstanceIdentifier": "sample-instance-2",
                    "IsClusterWriter": true,
                    "DBClusterParameterGroupStatus": "in-sync",
                    "PromotionTier": 1
                },

            ],
            "VpcSecurityGroups": [
                {
                    "VpcSecurityGroupId": "sg-9084c2ec",
                    "Status": "active"
                }
            ],
            "HostedZoneId": "Z06853723JYKYBXTJ49RB",
            "StorageEncrypted": false,
            "DbClusterResourceId": "cluster-T4LGLANHVAPGQYYULWUDKLVQL4",
            "DBClusterArn": "arn:aws:rds:us-east-1:123456789012:cluster:sample-
cluster",
            "AssociatedRoles": [],
            "IAMDatabaseAuthenticationEnabled": false,
            "ClusterCreateTime": "2023-11-06T18:05:41.568000+00:00",
            "EngineMode": "provisioned",
            "DeletionProtection": false,
            "HttpEndpointEnabled": false,
            "CopyTagsToSnapshot": false,
            "CrossAccountClone": false,
            "DomainMemberships": [],
            "TagList": [],
            "StorageType": "iopt1",
            "AutoMinorVersionUpgrade": false,
            "NetworkType": "IPV4",
            "IOOptimizedNextAllowedModificationTime":
 "2023-12-07T18:05:41.580000+00:00"
        }
    ]
}
```

Example

Ejemplo 3: mostrar detalles específicos de un clúster de Amazon DocumentDB

Para enumerar un subconjunto de los detalles de los clústeres mediante el AWS CLI, añada un elemento `--query` que especifique los miembros del clúster que se van a enumerar en

la `describe-db-clusters` operación. El parámetro de `--db-cluster-identifier` es el identificador del clúster concreto del que desea mostrar los detalles. Para obtener más información sobre consultas, consulte Cómo filtrar la salida con la opción `--query` en la Guía de usuario de AWS Command Line Interface .

En el siguiente ejemplo de la se muestran las instancias de un clúster de Amazon DocumentDB.

Para Linux, macOS o Unix:

```
aws docdb describe-db-clusters \
    --filter Name=engine,Values=docdb \
    --db-cluster-identifier sample-cluster \
    --query 'DBClusters[*].[DBClusterMembers]'
```

Para Windows:

```
aws docdb describe-db-clusters ^
    --filter Name=engine,Values=docdb ^
    --db-cluster-identifier sample-cluster ^
    --query 'DBClusters[*].[DBClusterMembers]'
```

La salida de esta operación será similar a lo que se indica a continuación.

```
[
    [
        [
            {
                "DBInstanceIdentifier": "sample-instance-1",
                "IsClusterWriter": true,
                "DBClusterParameterGroupStatus": "in-sync",
                "PromotionTier": 1
            },
            {
                "DBInstanceIdentifier": "sample-instance-2",
                "IsClusterWriter": false,
                "DBClusterParameterGroupStatus": "in-sync",
                "PromotionTier": 1
            }
        ]
    ]
]
```

Modificación de un clúster de Amazon DocumentDB

Para modificar un clúster, el clúster debe tener el estado available (disponible). No puede modificar un clúster que está detenido. Si el clúster está detenido, inicie primero el clúster, espere a que el clúster esté disponible y, a continuación, realice las modificaciones deseadas. Para obtener más información, consulte Detención e inicio de un clúster de bases de datos de Amazon DocumentDB.

Using the Consola de administración de AWS

Utilice el siguiente procedimiento para modificar un clúster de Amazon DocumentDB específico mediante la consola.

Modificación de un clúster de Amazon DocumentDB

1. Inicie sesión en y abra la Consola de administración de AWS consola de Amazon DocumentDB en https://console.aws.amazon.com /docdb.
2. En el panel de navegación, seleccione Clusters (Clústeres).

   > **Tip**
   >
   > Si no ve el panel de navegación del lado izquierdo de la pantalla, seleccione el icono de menú
   > (≡)
   > en la esquina superior izquierda de la página.

3. Especifique el clúster que desee modificar seleccionando el botón situado a la izquierda del nombre del clúster.
4. Elija Actions (Acciones) y después Modify (Modificar).
5. En el panel Modify Cluster: <cluster-name> (Modificar clúster: <nombre-clúster>, realice los cambios que desee. Puede realizar cambios en las siguientes áreas:

   - Especificaciones del clúster: nombre del clúster, grupos de seguridad y administración de credenciales.
   - Configuración del almacenamiento en clúster: el modo de almacenamiento de datos del clúster. Elija entre configuración estándar u optimizada para E/S.
   - Opciones del clúster: el grupo de parámetros y el puerto del clúster.
   - Copia de seguridad: el período de copia de seguridad y de retención de la copia de seguridad del clúster.

- Exportación de registros: permite habilitar o deshabilitar los registros de auditoría o perfiles de exportación.
- Mantenimiento: permite establecer la ventana de mantenimiento del clúster.
- Protección de eliminación: permite habilitar o deshabilitar la protección de eliminación en el clúster. La protección contra eliminación está habilitada de forma predeterminada.

6. Cuando haya terminado, elija Continuar para ver un resumen de los cambios.
7. Si está satisfecho con los cambios, puede elegir Modificar clúster para modificar el clúster. También puede elegir Atrás o Cancelar para editar o cancelar los cambios, respectivamente.

Los cambios pueden tardar unos minutos en aplicarse. Solo se puede usar el clúster cuando su estado sea available (disponible). Puede monitorizar el estado del clúster mediante la consola o la AWS CLI. Para obtener más información, consulte Supervisión del estado de un clúster de Amazon DocumentDB.

Using the AWS CLI

Utilice la operación `modify-db-cluster` para modificar el clúster especificado mediante la AWS CLI. Para obtener más información, consulte `ModifyDBCluster` en la Referencia de la API de Amazon DocumentDB.

Parameters

- **`--db-cluster-identifier`**: obligatorio. El identificador del clúster de Amazon DocumentDB que va a modificar.
- **`--backup-retention-period`**: opcional. El número de días durante los que se retienen las copias de seguridad automatizadas. Los valores válidos están comprendidos entre 1 y 35.
- **`--storage-type`**: opcional. Configuración de almacenamiento en clústeres. Los valores válidos son `standard` (estándar) o `iopt1` (optimizado para E/S).
- **`--db-cluster-parameter-group-name`**: opcional. El nombre del grupo de parámetros de clúster que se va a usar para el clúster.
- **`--manage-master-user-password`**: opcional. Amazon DocumentDB genera la contraseña del usuario maestro y la administra durante todo su ciclo de vida en Secrets Manager.
- **`--rotate-master-user-password`**: opcional. Secrets Manager genera una nueva versión de secreto para el secreto existente. La nueva versión del secreto contiene la nueva contraseña de usuario principal. Amazon DocumentDB cambia la contraseña del usuario principal para el clúster para que coincida con la contraseña de la nueva versión del secreto.

Debe especificar la opción **`--apply-immediately`** cuando rota la contraseña principal.

- **`--master-user-password`**: opcional. La nueva contraseña del usuario de la base de datos principal.

  Restricciones para la contraseña:

  - La longitud es de 8 a 100 caracteres ASCII imprimibles.
  - Se puede utilizar cualquier carácter ASCII imprimible, excepto los siguientes:
    - **`/`** (barra inclinada)
    - **`"`** (comillas dobles)
    - **`@`** (símbolo de arroba)
- **`--new-db-cluster-identifier`**: opcional. El nuevo identificador del clúster cuando se cambia el nombre de un clúster. Este valor se almacena como una cadena en minúsculas.

  Restricciones en la nomenclatura:

  - Debe tener [1-63] letras, números o guiones.
  - El primer carácter debe ser una letra.
  - No puede terminar con un guion ni contener dos guiones consecutivos.
  - Debe ser único para todos los clústeres de Amazon RDS, Amazon Neptune y Amazon DocumentDB por región. Cuenta de AWS
- **`--preferred-backup-window`**: opcional. El intervalo de tiempo diario (en Tiempo Universal Coordinado [UTC]) durante el cual se crean copias de seguridad automatizadas.
  - Formato: `hh24:mm-hh24:mm`
- **`--preferred-maintenance-window`**: opcional. El intervalo de tiempo semanal (en UTC) durante el cual puede llevarse a cabo el mantenimiento del sistema.
  - Formato: `ddd:hh24:mm-ddd:hh24:mm`
  - Días válidos: `Sun`, `Mon`, `Tue`, `Wed`, `Thu`, `Fri` y `Sat`.
- **`--deletion-protection`** o **`--no-deletion-protection`**: opcional. Si la protección contra eliminación se debe habilitar en este clúster. La protección contra eliminación evita que el clúster se elimine accidentalmente hasta que se modifique para deshabilitar la protección contra eliminación. Para obtener más información, consulte Eliminación de un clúster de Amazon DocumentDB.

- **`--apply-immediately`** o **`--no-apply-immediately`**: utilice `--apply-immediately` para aplicar los cambios inmediatamente. Utilice `--no-apply-immediately` para aplicar el cambio durante el próximo periodo de mantenimiento de su clúster.

Example

El siguiente código cambia el periodo de retención de copia de seguridad del clúster `sample-cluster`.

Para Linux, macOS o Unix:

```
aws docdb modify-db-cluster \
       --db-cluster-identifier sample-cluster \
       --apply-immediately \
       --backup-retention-period 7
```

Para Windows:

```
aws docdb modify-db-cluster ^
       --db-cluster-identifier sample-cluster ^
       --apply-immediately ^
       --backup-retention-period 7
```

La salida de esta operación será similar a lo que se indica a continuación.

```
{
    "DBCluster": {
        "BackupRetentionPeriod": 7,
        "DbClusterResourceId": "cluster-VDP53QEWST7YHM36TTXOPJT5YE",
        "Status": "available",
        "DBClusterMembers": [
            {
                "PromotionTier": 1,
                "DBClusterParameterGroupStatus": "in-sync",
                "DBInstanceIdentifier": "sample-cluster-instance",
                "IsClusterWriter": true
            }
        ],
        "ReadReplicaIdentifiers": [],
        "AvailabilityZones": [
```

```
            "us-east-1b",
            "us-east-1c",
            "us-east-1a"
        ],
        "ReaderEndpoint": "sample-cluster.cluster-ro-ctevjxdlur57.us-
east-1.rds.amazonaws.com",
        "DBClusterArn": "arn:aws:rds:us-east-1:123456789012:cluster:sample-cluster",
        "PreferredMaintenanceWindow": "sat:09:51-sat:10:21",
        "EarliestRestorableTime": "2018-06-17T00:06:19.374Z",
        "StorageEncrypted": false,
        "MultiAZ": false,
        "AssociatedRoles": [],
        "MasterUsername": "<your-master-user-name>",
        "DBClusterIdentifier": "sample-cluster",
        "VpcSecurityGroups": [
            {
                "Status": "active",
                "VpcSecurityGroupId": "sg-77186e0d"
            }
        ],
        "HostedZoneId": "Z2SUY0A1719RZT",
        "LatestRestorableTime": "2018-06-18T21:17:05.737Z",
        "AllocatedStorage": 1,
        "Port": 27017,
        "Engine": "docdb",
        "DBClusterParameterGroup": "default.docdb3.4",
        "Endpoint": "sample-cluster.cluster-ctevjxdlur57.us-
east-1.rds.amazonaws.com",
        "DBSubnetGroup": "default",
        "PreferredBackupWindow": "00:00-00:30",
        "EngineVersion": "3.4",
        "ClusterCreateTime": "2018-06-06T19:25:47.991Z",
        "IAMDatabaseAuthenticationEnabled": false
    }
}
```

Los cambios pueden tardar unos minutos en aplicarse. Solo se puede usar el clúster cuando su estado sea available (disponible). Puede monitorizar el estado del clúster mediante la consola o la AWS CLI. Para obtener más información, consulte Supervisión del estado de un clúster de Amazon DocumentDB.

Determinación de las tareas de mantenimiento pendientes

Para saber si tiene la versión del motor de Amazon DocumentDB más reciente, determine si hay pendientes tareas de mantenimiento del clúster.

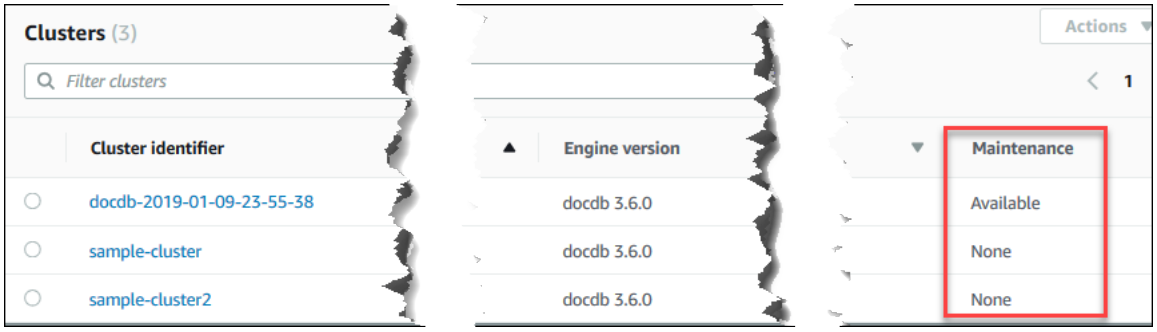
Using the Consola de administración de AWS

Puede usarlo Consola de administración de AWS para determinar si un clúster tiene tareas pendientes de mantenimiento.

1. Inicie sesión en y abra la Consola de administración de AWS consola de Amazon DocumentDB en https://console.aws.amazon.com /docdb.
2. En el panel de navegación, seleccione Clusters (Clústeres).

   > **Tip**
   >
   > Si no ve el panel de navegación del lado izquierdo de la pantalla, seleccione el icono de menú
   > (≡)
   > en la esquina superior izquierda de la página.

3. Localice la columna Maintenance (Mantenimiento) para determinar si un clúster tiene tareas de mantenimiento pendientes.



   None (Ninguno) indica que el clúster está ejecutando la versión más reciente del motor. Available (Disponible) indica que el clúster tiene pendientes tareas de mantenimiento, lo que podría significar que es necesario realizar una actualización del motor.

4. Si el clúster tiene pendientes tareas de mantenimiento, continúe con los pasos que se indican en Actualización de un parche a la versión del motor de un clúster.

Using the AWS CLI

Puede utilizarla AWS CLI para determinar si un clúster tiene la última versión del motor mediante la `describe-pending-maintenance-actions` operación con los siguientes parámetros.

Parameters

- **`--resource-identifier`**: opcional. El ARN del recurso (clúster). Si este parámetro se omite, se enumeran las operaciones de mantenimiento pendientes de todos los clústeres.
- **`--region`**: opcional. La región de AWS en la que desea ejecutar esta operación, por ejemplo, `us-east-1`.

Example

Para Linux, macOS o Unix:

```
aws docdb describe-pending-maintenance-actions \
   --resource-identifier arn:aws:rds:us-east-1:123456789012:cluster:sample-cluster \
   --region us-east-1
```

Para Windows:

```
aws docdb describe-pending-maintenance-actions ^
   --resource-identifier arn:aws:rds:us-east-1:123456789012:cluster:sample-cluster ^
   --region us-east-1
```

La salida de esta operación será similar a lo que se indica a continuación.

```
{
    "PendingMaintenanceActions": [
        {
            "ResourceIdentifier": "arn:aws:rds:us-
east-1:123456789012:cluster:sample-cluster",
            "PendingMaintenanceActionDetails": [
                {
                    "Description": "New feature",
                    "Action": "db-upgrade",
                    "ForcedApplyDate": "2019-02-25T21:46:00Z",
```

```
                    "AutoAppliedAfterDate": "2019-02-25T07:41:00Z",
                    "CurrentApplyDate": "2019-02-25T07:41:00Z"
                }
            ]
        }
    ]
}
```

Si el clúster tiene pendientes tareas de mantenimiento, continúe con los pasos que se indican en Actualización de un parche a la versión del motor de un clúster.

Actualización de un parche a la versión del motor de un clúster

En esta sección, explicaremos cómo implementar una actualización de parche mediante el Consola de administración de AWS o el AWS CLI. Una actualización de parche es una actualización dentro de la misma versión del motor (por ejemplo, la actualización de una versión del motor 3.6 a una versión del motor 3.6 más reciente). Puede actualizarla inmediatamente o durante el próximo periodo de mantenimiento del clúster. Para determinar si el motor necesita una actualización, consulte Determinación de las tareas de mantenimiento pendientes. Tenga en cuenta que, al aplicar la actualización, su clúster sufrirá algún tiempo de inactividad.

> **Note**
>
> Si está intentando actualizar desde una versión principal del motor a otra, como de la 3.6 a la 5.0, consulte Actualización local de la versión principal Amazon DocumentDB o Actualización del clúster de Amazon DocumentDB mediante AWS Database Migration Service. Una actualización local de la versión principal solo admite docdb 5.0 como versión del motor de destino.

Existen dos requisitos de configuración para obtener las actualizaciones de parches más recientes para la versión del motor de un clúster:

- El estado del clúster debe ser disponible.
- El clúster debe estar ejecutando una versión del motor más antigua.

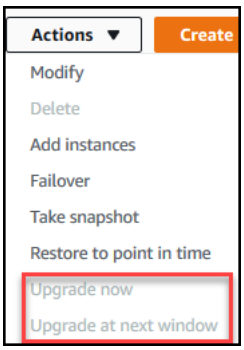
Using the Consola de administración de AWS

El siguiente procedimiento actualiza los parches de la versión del motor de su clúster a la versión más reciente con la consola. Puede actualizarla inmediatamente o durante el próximo periodo de mantenimiento del clúster.

1. Inicie sesión en y abra la Consola de administración de AWS consola de Amazon DocumentDB en https://console.aws.amazon.com /docdb.
2. En el panel de navegación, seleccione Clusters (Clústeres). En la lista de clústeres, elija el botón situado a la izquierda del clúster que desee actualizar. El estado del clúster debe ser disponible.

   > **Tip**
   >
   > Si no ve el panel de navegación del lado izquierdo de la pantalla, seleccione el icono de menú
   > (≡)
   > en la esquina superior izquierda de la página.

3. En el menú Actions (Acciones), elija una de las opciones siguientes. Estas opciones de menú solo se pueden seleccionar si en el clúster elegido no se está ejecutando la última versión del motor.

   - Actualizar ahora: inicia inmediatamente el proceso de actualización. El clúster se quedará sin conexión durante un tiempo mientras se actualiza a la última versión del motor.
   - Actualizar en el siguiente periodo: inicia el proceso de actualización durante el próximo periodo de mantenimiento del clúster. El clúster se quedará sin conexión durante un tiempo mientras se actualiza a la última versión del motor.

4. Cuando se abra la ventana de confirmación, seleccione una de las siguientes opciones:

- Actualizar: para actualizar el clúster a la última versión del motor de acuerdo con el plan elegido en el paso anterior.
- Cancelar: para cancelar la actualización del motor del clúster y continuar con la versión actual del motor del clúster.

Using the AWS CLI

Puede aplicar actualizaciones de parches a su clúster mediante la `apply-pending-maintenance-action` operación AWS CLI y con los siguientes parámetros.

Parameters

- **`--resource-identifier`**: obligatorio. El ARN del clúster de Amazon DocumentDB que va a actualizar.
- **`--apply-action`**: obligatorio. Se permiten los siguientes valores. Para actualizar la versión de su motor de clúster, utilice `db-upgrade`.
  - **`db-upgrade`**
  - **`system-update`**
- **`--opt-in-type`**: obligatorio. Se permiten los siguientes valores.
  - `immediate`: aplicar inmediatamente la acción de mantenimiento.
  - `next-maintenance`: aplicar la operación de mantenimiento durante el siguiente período de mantenimiento.
  - `undo-opt-in`: cancelar todas las solicitudes de alta `next-maintenance` existentes.

Example

En el siguiente ejemplo se actualiza la versión del motor de `sample-cluster` a la versión 4.0.0.

Para Linux, macOS o Unix:

```
aws docdb apply-pending-maintenance-action \
   --resource-identifier arn:aws:rds:us-east-1:123456789012\:cluster:sample-cluster
 \
   --apply-action db-upgrade \
   --opt-in-type immediate
```

Para Windows:

```
aws docdb apply-pending-maintenance-action ^
   --resource-identifier arn:aws:rds:us-east-1:123456789012:cluster:sample-cluster ^
   --apply-action db-upgrade ^
   --opt-in-type immediate
```

El resultado de esta operación será similar a lo que se indica a continuación:

```
{
    "ResourcePendingMaintenanceActions": {
        "ResourceIdentifier": "arn:aws:rds:us-
east-1:444455556666:cluster:docdb-2019-01-09-23-55-38",
        "PendingMaintenanceActionDetails": [
            {
                "CurrentApplyDate": "2019-02-20T20:57:06.904Z",
                "Description": "Bug fixes",
                "ForcedApplyDate": "2019-02-25T21:46:00Z",
                "OptInStatus": "immediate",
                "Action": "db-upgrade",
                "AutoAppliedAfterDate": "2019-02-25T07:41:00Z"
            }
        ]
    }
}
```

Detención e inicio de un clúster de bases de datos de Amazon DocumentDB

La detención e inicio de los clústeres de Amazon DocumentDB puede ayudarle a administrar los costos de entornos de desarrollo y pruebas. En lugar de crear y eliminar clústeres y las instancias cada vez que utilice Amazon DocumentDB, puede detener temporalmente todas las instancias en el clúster cuando ya no son necesarias. A continuación, puede iniciarlos de nuevo cuando reanude sus pruebas.

Temas

- Información general de detención e inicio de un clúster
- Operaciones que puede llevar a cabo en un clúster detenido

Información general de detención e inicio de un clúster

Durante los periodos en los que no necesite un clúster de Amazon DocumentDB, puede detener todas las instancias de ese clúster a la vez. A continuación, puede volver a iniciar el clúster en cualquier momento que necesite usarlo. El inicio y la detención simplifican los procesos de configuración y eliminación de clústeres usados para desarrollo, pruebas o actividades similares que no requieren disponibilidad continua. Puede detener e iniciar un clúster con Consola de administración de AWS o AWS CLI con una sola acción, independientemente del número de instancias que haya en el clúster.

Aunque el clúster se detenga, el volumen de almacenamiento del clúster permanece sin cambios. Solo se le cobrará el almacenamiento, las instantáneas manuales y el almacenamiento de la copia de seguridad automática dentro de su intervalo de retención especificado. No se le cobrarán las horas de ninguna instancia. Después de siete días, Amazon DocumentDB vuelve a iniciar automáticamente el clúster de base de datos para asegurarse de llevar a cabo las actualizaciones de mantenimiento necesarias. Cuando el clúster comience después de siete días, se le comenzará a cobrar las instancias en el clúster de nuevo. Cuando el clúster se detenga, no podrá consultar el volumen de almacenamiento, ya que la consulta requiere que las instancias estén disponibles.

Cuando se detiene un clúster de Amazon DocumentDB, ni el clúster ni sus instancias se pueden modificar en modo alguno. Esto incluye añadir o eliminar instancias o eliminar el clúster.

Using the Consola de administración de AWS

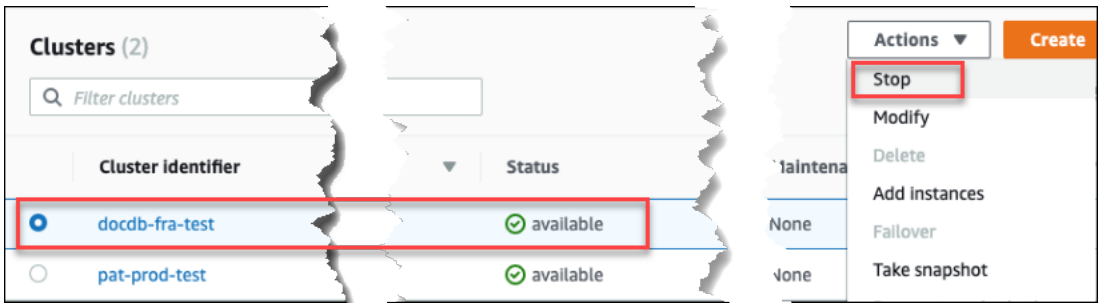
El procedimiento siguiente le muestra cómo detener un clúster con una o varias instancias en un estado disponible o iniciar un clúster detenido.

Detención o inicio de un clúster de Amazon DocumentDB

1. Inicie sesión en y abra la Consola de administración de AWS consola de Amazon DocumentDB en https://console.aws.amazon.com /docdb.
2. En el panel de navegación, seleccione Clusters (Clústeres).

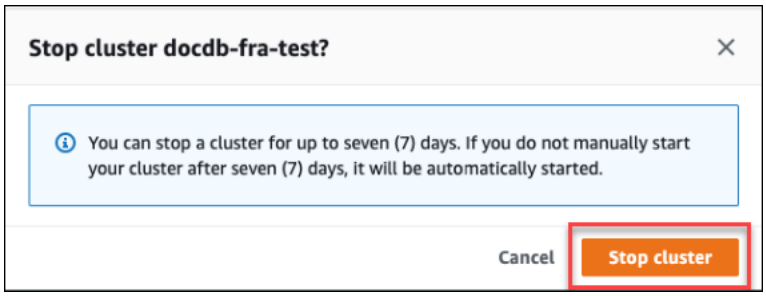
> **Tip**
>
> Si no ve el panel de navegación del lado izquierdo de la pantalla, seleccione el icono de menú
> (≡)
> en la esquina superior izquierda de la página.

3. En la lista de clústeres, elija el botón situado a la izquierda del nombre del clúster que quiera detener o iniciar.
4. Elija Actions (Acciones) y, a continuación, elija la acción que desea realizar en el clúster.
   - Si desea detener el clúster y el clúster está disponible:
     a. Elija Detener.

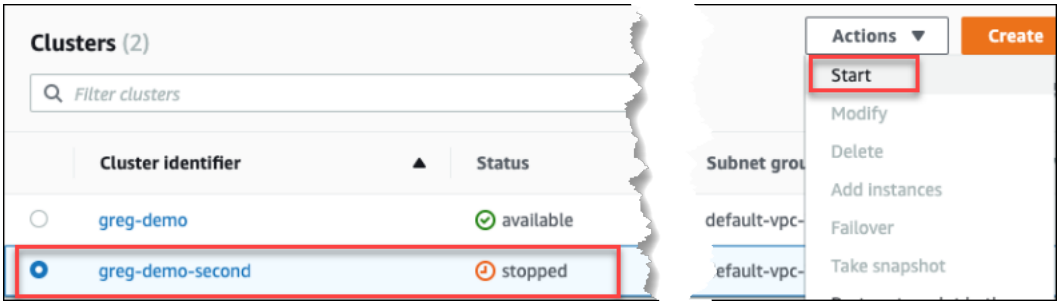


Para evitar la activación del mecanismo de activación por error, la operación de detención para primero las instancias de réplica y, a continuación, la instancia principal.

     b. En el cuadro de diálogo de confirmación, acepte que desea detener el clúster seleccionado Stop cluster (Detener clúster) o mantenga el clúster en ejecución mediante Cancel (Cancelar).



   - Si desea iniciar el clúster y este se detiene, seleccione Start (Iniciar).



5. Monitorice el estado del clúster y sus instancias. Si ha iniciado el clúster, podrá volver a utilizar el clúster cuando este y sus instancias estén disponibles. Para obtener más información, consulte Determinación del estado de un clúster.



Using the AWS CLI

Los siguientes ejemplos de código le muestras cómo detener un clúster con una o varias instancias en un estado disponible o iniciar un clúster detenido.

Para detener un clúster con una o más instancias disponibles mediante el AWS CLI, utilice la operación. `stop-db-cluster` Para iniciar un clúster detenido, utilice la operación `start-db-cluster`. En ambas operaciones se utiliza el parámetro `--db-cluster-identifier`.

Parámetro

- **`--db-cluster-identifier`**: obligatorio. El nombre del clúster que detener e iniciar.

Example — Para detener un clúster mediante el AWS CLI

El siguiente código detiene el clúster `sample-cluster`. El clúster debe tener una o más instancias en un estado disponible.

Para Linux, macOS o Unix:

```
aws docdb stop-db-cluster \
   --db-cluster-identifier sample-cluster
```

Para Windows:

```
aws docdb stop-db-cluster ^
   --db-cluster-identifier sample-cluster
```

Example — Para iniciar un clúster mediante el AWS CLI

El siguiente código inicia el clúster `sample-cluster`. El clúster debe estar detenido actualmente.

Para Linux, macOS o Unix:

```
aws docdb start-db-cluster \
   --db-cluster-identifier sample-cluster
```

Para Windows:

```
aws docdb start-db-cluster ^
   --db-cluster-identifier sample-cluster
```

Operaciones que puede llevar a cabo en un clúster detenido

Mientras un clúster de Amazon DocumentDB esté detenido, puede realizar una point-in-time restauración en cualquier punto dentro del período de retención de copias de seguridad automatizado especificado. Para obtener más información sobre cómo realizar una point-in-time restauración, consulteRestauración a un momento dado.

No se puede modificar la configuración de un clúster de Amazon DocumentDB ni de ninguna de sus instancias mientras el clúster esté detenido. Tampoco puede añadir ni quitar instancias del clúster, ni eliminar el clúster si todavía tiene alguna instancia asociada. Debe iniciar el clúster antes de realizar cualquier tarea administrativa de ese tipo.

Amazon DocumentDB aplica cualquier mantenimiento programado a su clúster detenido solo después de que se vuelva a iniciar. Después de siete días, Amazon DocumentDB inicia automáticamente un clúster detenido para que no se quede demasiado rezagado en su estado de mantenimiento. Cuando el clúster se reinicie, se le comenzará a cobrar las instancias en el clúster de nuevo.

Cuando un clúster está detenido, Amazon DocumentDB no realiza los copias de seguridad automatizadas ni amplía el período de retención de copia de seguridad.

Eliminación de un clúster de Amazon DocumentDB

Puede eliminar un clúster de Amazon DocumentDB mediante el Consola de administración de AWS o el. AWS CLI Para eliminar un clúster, el clúster debe tener el estado disponible y no debe tener

ninguna instancia asociada a él. Si el clúster está detenido, inicie primero el clúster, espere a que el clúster esté disponible, y, a continuación, elimine el clúster. Para obtener más información, consulte Detención e inicio de un clúster de bases de datos de Amazon DocumentDB.

Protección contra eliminación

Para proteger su clúster contra la eliminación accidental, puede habilitar la protección contra eliminación. La protección contra eliminación se habilita de forma predeterminada cuando crea un clúster mediante la consola. Sin embargo, la protección contra eliminación está deshabilitada de forma predeterminada si crea un clúster con la AWS CLI.

Amazon DocumentDB aplica la protección contra eliminación para un clúster si realiza la operación de eliminación mediante la consola o la AWS CLI. Si la protección contra eliminación está habilitada, no podrá eliminar un clúster. Para eliminar un clúster con la protección contra eliminación habilitada, primero debe modificar el clúster y deshabilitar la protección contra eliminación.

Cuando use la consola con la protección contra eliminación habilitada en un clúster, no podrá eliminar la última instancia del clúster, ya que también se eliminará el clúster. Puede eliminar la última instancia de un clúster con protección contra eliminación con la AWS CLI. Sin embargo, el propio clúster sigue existiendo y se conservan los datos. Puede acceder a los datos mediante la creación de nuevas instancias para el clúster. Para obtener más información sobre cómo habilitar y deshabilitar la protección contra eliminación, consulte:

- Creación de un clúster de Amazon DocumentDB
- Modificación de un clúster de Amazon DocumentDB

Using the Consola de administración de AWS

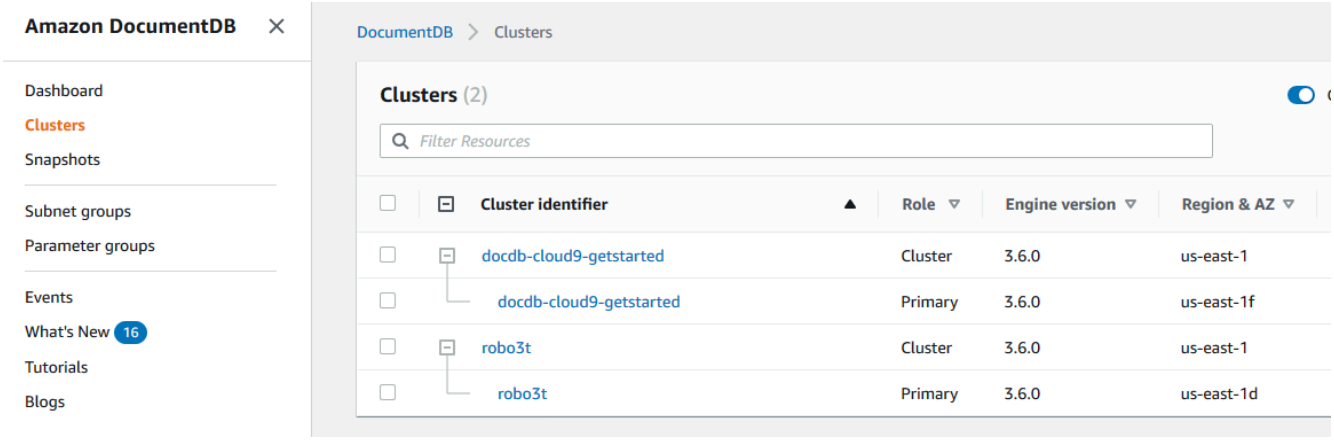
Para eliminar un clúster mediante el Consola de administración de AWS, la protección de eliminación debe estar deshabilitada.

Para determinar si un clúster tiene habilitada la protección contra eliminación, realice el siguiente procedimiento:

1. Inicie sesión en y abra la Consola de administración de AWS consola de Amazon DocumentDB en https://console.aws.amazon.com /docdb.
2. En el panel de navegación, seleccione Clusters (Clústeres).

> **Tip**
>
> Si no ve el panel de navegación del lado izquierdo de la pantalla, seleccione el icono de menú
> (≡)
> en la esquina superior izquierda de la página.

3. Tenga en cuenta que en el cuadro de navegación de clústeres, la columna Identificador de clústeres muestra tanto los clústeres como las instancias. Las instancias se muestran en clústeres, de forma similar a la siguiente captura de pantalla.



4. Elija el nombre del clúster y seleccione la pestaña Configuración. En la sección Detalles del clúster busque Protección contra eliminación. Si la protección contra eliminación está habilitada, modifique el clúster para deshabilitar la protección contra eliminación. Para obtener más información sobre la modificación de un clúster, consulte Modificación de un clúster de Amazon DocumentDB.

   Una vez que se deshabilite la protección contra eliminación, podrá eliminar el clúster.

Para eliminar un clúster:

1. En el panel de navegación, seleccione Clusters (Clústeres).
2. Determine si el clúster tiene alguna instancia; para ello, compruebe la columna Identificador de clústeres para determinar si aparecen las instancias enumeradas a continuación. Para poder eliminar un clúster, debe eliminar todas sus instancias. Para obtener más información, consulte Eliminación de una instancia de Amazon DocumentDB.
3. Si su clúster dispone de instancias, realice uno de los siguientes pasos.

- Si el clúster no tiene instancias, seleccione el botón situado a la izquierda del nombre del clúster y elija Acciones. En el menú desplegable, seleccione Eliminar. Complete el cuadro de diálogo Delete <cluster-name> (Eliminar <nombre de clúster>) y, a continuación, elija Delete (Eliminar).
- Si el clúster tiene una o varias instancias, haga lo siguiente:

  a. En el panel de navegación, seleccione Clusters (Clústeres).

  b. Elimine cada una de las instancias del clúster. Para ello, seleccione la casilla de verificación situada a la izquierda del nombre del clúster. Seleccione Acciones y, a continuación, elija Eliminar. Complete el cuadro de diálogo Delete <cluster-name> (Eliminar <nombre de clúster>) y, a continuación, elija Delete (Eliminar).

  Cuando elimine la última instancia, el clúster también se eliminará. Para obtener más información sobre la eliminación de instancias, consulte Eliminación de una instancia de Amazon DocumentDB.

La eliminación del clúster puede tardar varios minutos. Para monitorizar el estado del clúster, consulte Supervisión del estado de un clúster de Amazon DocumentDB.

Using the AWS CLI

No puede eliminar un clúster que tenga instancias asociadas. Para determinar qué instancias están asociadas al clúster, ejecute el comando `describe-db-clusters` y elimine todas las instancias del clúster. A continuación, si es necesario, deshabilite la protección contra eliminación de su clúster y, por último, elimine el clúster.

1. En primer lugar, elimine todas las instancias del clúster.

   Para determinar qué instancias necesita eliminar, ejecute el siguiente comando.

   ```
   aws docdb describe-db-clusters \
       --db-cluster-identifier sample-cluster \
       --query 'DBClusters[*].
   [DBClusterIdentifier,DBClusterMembers[*].DBInstanceIdentifier]'
   ```

   La salida de esta operación será similar a lo que se indica a continuación (formato JSON).

   ```
   [
       [
   ```

```
        "sample-cluster",
        [
            "sample-instance-1",
            "sample-instance-2"
        ]
    ]
]
```

Si el clúster que desea eliminar tiene instancias, elimínelas como se muestra a continuación.

```
aws docdb delete-db-instance \
    --db-instance-identifier sample-instance
```

2. En segundo lugar, deshabilite la protección contra eliminación.

   El uso de AWS CLI para eliminar todas las instancias de un clúster no elimina el clúster. También debe eliminar el clúster, pero puede hacerlo solo si se deshabilita la protección contra eliminación.

   Para determinar si el clúster tiene la protección contra eliminación habilitada, ejecute el siguiente comando.

   > **Tip**
   >
   > Para ver el estado de la protección contra eliminación de todos los clústeres de Amazon DocumentDB, omita el parámetro `--db-cluster-identifier`.

```
aws docdb describe-db-clusters \
    --db-cluster-identifier sample-cluster \
    --query 'DBClusters[*].[DBClusterIdentifier,DeletionProtection]'
```

La salida de esta operación será similar a lo que se indica a continuación.

```
[
    [
        "sample-cluster",
        "true"
    ]
```

```
]
```

Si el clúster tiene la protección contra eliminación habilitada, modifique el clúster y deshabilite la protección contra eliminación. Para deshabilitar la protección contra eliminación en el clúster, ejecute el siguiente comando.

```
aws docdb modify-db-cluster \
    --db-cluster-identifier sample-cluster \
    --no-deletion-protection \
    --apply-immediately
```

3. Por último, elimine el clúster.

   Una vez que la protección contra eliminación esté deshabilitada, podrá eliminar el clúster. Para eliminar un clúster, utilice la operación `delete-db-cluster` con los siguientes parámetros.

   - **`--db-cluster-identifier`**: obligatorio. El identificador del clúster que desee eliminar.
   - **`--final-db-snapshot-identifier`**: opcional. Si desea una instantánea final, debe incluir este parámetro con un nombre para la instantánea final. Debe incluir `--final-db-snapshot-identifier` o `--skip-final-snapshot`.

     Restricciones en la nomenclatura:

     - Debe tener [1-63] letras, números o guiones.
     - El primer carácter debe ser una letra.
     - No puede terminar con un guion ni contener dos guiones consecutivos.
     - Debe ser único para todos los clústeres de Amazon RDS, Amazon Neptune y Amazon DocumentDB por región. Cuenta de AWS
   - **`--skip-final-snapshot`**: opcional. Use este parámetro solo si no desea realizar una instantánea final antes de eliminar el clúster. El comportamiento predeterminado es realizar una instantánea final. Debe incluir `--final-db-snapshot-identifier` o `--skip-final-snapshot`.

El siguiente AWS CLI código elimina el clúster `sample-cluster` con una instantánea final. La operación genera un error si hay las instancias asociadas al clúster o si está habilitada la protección contra eliminación.

Example

Para Linux, macOS o Unix:

```
aws docdb delete-db-cluster \
    --db-cluster-identifier sample-cluster \
    --final-db-snapshot-identifier sample-cluster-final-snapshot
```

Para Windows:

```
aws docdb delete-db-cluster ^
    --db-cluster-identifier sample-cluster ^
    --final-db-snapshot-identifier sample-cluster-final-snapshot
```

Example

El siguiente AWS CLI código elimina el clúster `sample-cluster` sin tomar una instantánea final.

Para Linux, macOS o Unix:

```
aws docdb delete-db-cluster \
    --db-cluster-identifier sample-cluster \
    --skip-final-snapshot
```

Para Windows:

```
aws docdb delete-db-cluster ^
    --db-cluster-identifier sample-cluster ^
    --skip-final-snapshot
```

El resultado de la operación `delete-db-cluster` es el clúster que se va a eliminar.

La eliminación del clúster puede tardar varios minutos. Para monitorizar el estado del clúster, consulte Monitorización del estado de un clúster.

Escalado de clústeres de Amazon DocumentDB

Amazon DocumentDB le permite escalar el almacenamiento y la computación en los clústeres en función de sus necesidades. En esta sección se describe cómo puede utilizar el escalado de almacenamiento, el escalado de instancia y el escalado de lectura para administrar el rendimiento y el escalado de los clústeres e instancias de Amazon DocumentDB.

Temas

- Escalado del almacenamiento
- Escalado de instancia
- Escalado de lectura
- Escalado de escritura

Escalado del almacenamiento

El almacenamiento de Amazon DocumentDB se escala automáticamente con los datos del volumen de clúster. A medida que crecen los datos, el almacenamiento del volumen de clúster aumenta en incrementos de 10 GiB hasta un máximo de 128 TiB.

Escalado de instancia

Puede escalar el clúster de base de datos de Amazon DocumentDB como considere necesario modificando la clase de instancia de base de datos para cada instancia de base de datos del clúster de base de datos. Amazon DocumentDB admite varias clases de instancias que están optimizadas para Amazon DocumentDB.

Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon DocumentDB.

Escalado de lectura

Puede realizar el escalado de lectura de su clúster de Amazon DocumentDB creando un máximo de 15 réplicas de Amazon DocumentDB en el clúster. Cada réplica de Amazon DocumentDB devuelve los mismos datos del volumen de clúster con un retardo de réplica mínimo, normalmente menos de

100 milisegundos una vez que la instancia principal ha escrito una actualización. A medida que el tráfico de lectura aumenta, puede crear réplicas de Amazon DocumentDB adicionales y conectarlas directamente para distribuir la carga de lectura del clúster de base de datos. Las réplicas de Amazon DocumentDB no tienen que ser de la misma clase de instancia de base de datos que la instancia principal.

Para obtener más información, consulte Agregación de una instancia de Amazon DocumentDB a un clúster.

Para escalar las lecturas con Amazon DocumentDB, recomendamos que se conecte al clúster como conjunto de réplicas y distribuya las lecturas a las instancias de réplica mediante las funciones integradas de preferencias de lectura del controlador. Para obtener más información, consulte Conexión a Amazon DocumentDB como conjunto de réplicas.

Escalado de escritura

Puede escalar la capacidad de escritura en el clúster de Amazon DocumentDB aumentando el tamaño de la instancia principal del clúster. En esta sección se proporcionan dos métodos para escalar la instancia principal del clúster en función de sus necesidades. La primera opción busca minimizar el impacto de la aplicación, pero requiere completar más pasos. La segunda opción optimiza la simplicidad ya que tiene menos pasos, pero conlleva el inconveniente de tener más impacto potencial en la aplicación.

En función de la aplicación, puede elegir cuál de los enfoques siguientes es el mejor en su caso. Para obtener más información sobre los tamaños y costos de instancias disponibles, consulte la página Precios de Amazon DocumentDB.

1. Optimizar para obtener una alta disponibilidad y rendimiento: si se conecta al clúster en el modo de conjunto de réplicas (recomendado), puede utilizar el siguiente proceso para minimizar el impacto en la aplicación al escalar la instancia principal. Este método minimiza el impacto porque mantiene el clúster en alta disponibilidad o por encima de ella y los destinos de escalado de lectura se agregan al clúster como instancias, en lugar de actualizarse en su lugar.

    a. Agregue una o varias réplicas del tipo de instancia mayor al clúster (consulte ???). Se recomienda que todas las réplicas sean del mismo tipo de instancia o mayor que la principal. Esto evita una reducción involuntaria en el rendimiento de escritura al conmutar por error a un tipo de instancia más pequeño. Para la mayoría de los clientes, esto significa duplicar temporalmente el número de instancias de su clúster y, a continuación, eliminar las réplicas más pequeñas después de completar el escalado.

b. Establezca el nivel de conmutación por error en todas las réplicas nuevas en prioridad cero, garantizando que una réplica del tipo de instancia más pequeño tenga la prioridad de conmutación por error más alta. Para obtener más información, consulte ???.

c. Inicie una conmutación por error manual, que promoverá una de las nuevas réplicas para que sea la instancia principal. Para obtener más información, consulte ???.

> **Note**
>
> Esto incurrirá en ~30 segundos de tiempo de inactividad para el clúster. Por favor, planifique en consecuencia.

d. Elimine todas las réplicas de un tipo de instancia menor que la nueva instancia principal del clúster.

e. Vuelva a establecer el nivel de conmutación por error de todas las instancias en la misma prioridad (normalmente, esto significa volver a establecerlas en 1).

Como ejemplo, suponga que tiene un clúster que contiene actualmente tres instancias `r5.large` (una principal y dos réplicas) y desea escalar a un tipo de instancia `r5.xlarge`. Para ello, primero agregaría tres instancias de réplica `r5.xlarge` al clúster y, a continuación, establecería el nivel de conmutación por error de las nuevas réplicas `r5.xlarge` en cero. A continuación, iniciaría una conmutación por error manual (entendiendo que su aplicación experimentará ~30 segundos de tiempo de inactividad). Una vez completada la conmutación por error, eliminaría las tres instancias `r5.large` del clúster, dejando el clúster escalado a instancias `r5.xlarge`.

Para ayudar a optimizar los costos, las instancias de Amazon DocumentDB se facturan en incrementos de un segundo con un cargo mínimo de 10 minutos a partir de la implementación de un cambio de estado que se pueda facturar, como la creación, la modificación o la eliminación de una instancia. Para obtener más información, consulte Optimización de costos en la documentación de prácticas recomendadas.

2. Optimizar la simplicidad: este enfoque optimiza la simplicidad. No expande ni contrae el clúster, pero podría reducir temporalmente la capacidad de lectura.

   Es posible que al cambiar la clase de instancia de una réplica, la instancia deje de atender las solicitudes durante un breve período de tiempo, desde unos pocos segundos a menos de 30 segundos. Si se conecta al clúster en el modo de conjunto de réplicas (recomendado), esto

reduciría su capacidad de lectura en una réplica (por ejemplo, hasta el 66 % de la capacidad en un clúster de 3 nodos o el 75 % de la capacidad en un clúster de 4 nodos, etc.) durante la operación de escalado.

a. Escale una de las instancias de réplica del clúster. Para obtener más información, consulte Administración de clases de instancias.

b. Espere hasta que la instancia esté disponible (consulte Supervisión del estado de un clúster de Amazon DocumentDB).

> **Note**
>
> Esto incurrirá en ~30 segundos de tiempo de inactividad para el clúster. Por favor, planifique en consecuencia.

c. Continúe ejecutando los pasos 1 y 2 hasta que se hayan escalado todas las instancias de réplicas, una por una.

d. Iniciar una conmutación por error manual. Esto promoverá una de las réplicas para que sea la instancia principal. Para obtener más información, consulte Conmutación por error a Amazon DocumentDB.

> **Note**
>
> Esto provocará un tiempo de inactividad de hasta 30 segundos para el clúster, aunque suele llevar menos tiempo. Por favor, planifique en consecuencia.

e. Escale la anterior instancia principal (que ahora es una réplica).

Clonación de un volumen de clúster de base de datos de Amazon DocumentDB

Con la clonación de Amazon DocumentDB, puede crear un nuevo clúster que utilice el mismo volumen de clúster de Amazon DocumentDB y tenga los mismos datos que el original. El proceso está diseñado para ser rápido y rentable. El nuevo clúster con su volumen de datos asociado se conoce como clon. La creación de un clon es más rápido y más eficiente en el espacio que copiar físicamente los datos mediante una técnica diferente, como la restauración de una instantánea.

Amazon DocumentDB admite la creación de un clon aprovisionado de Amazon DocumentDB a partir de un clúster de Amazon DocumentDB aprovisionado. Cuando crea un clon con una configuración de implementación diferente a la de origen, el clon se crea con la versión secundaria más reciente del motor de base de datos Amazon DocumentDB.

Cuando crea clones a partir de sus clústeres de Amazon DocumentDB, los clones se crean en su cuenta, la misma cuenta que posee AWS el clúster de Amazon DocumentDB de origen.

Temas

- Información general de la clonación de Amazon DocumentDB
- Limitaciones de la clonación de Amazon DocumentDB
- Cómo funciona la clonación de Amazon DocumentDB
- Creación de un clon de Amazon DocumentDB

Información general de la clonación de Amazon DocumentDB

Amazon DocumentDB utiliza un copy-on-write protocolo para crear un clon. Este mecanismo utiliza un espacio adicional mínimo para crear un clon inicial. Cuando se crea el clon por primera vez, Amazon DocumentDB guarda una sola copia de los datos que utiliza el clúster de base de datos de Amazon DocumentDB de origen y el nuevo clúster de base de datos de Amazon DocumentDB (clonado). El almacenamiento adicional solo se asigna cuando el clúster de base de datos de Amazon DocumentDB de origen o el clon del clúster de base de datos de Amazon DocumentDB realizan cambios en los datos (en el volumen de almacenamiento de Amazon DocumentDB). Para obtener más información sobre el copy-on-write protocolo, consulteCómo funciona la clonación de Amazon DocumentDB.

La clonación de Amazon DocumentDB es especialmente útil para configurar rápidamente entornos de prueba mediante sus datos de producción, sin riesgo de corrupción de datos. Puede utilizar clones para muchos tipos de aplicaciones de corta duración, como las siguientes:

- Experimente con cambios potenciales (por ejemplo, cambios de esquema y cambios de grupo de parámetros) para evaluar todos los impactos.
- Realice operaciones intensivas de carga de trabajo, como exportar datos o ejecutar consultas analíticas en el clon.
- Cree una copia del clúster de base de datos de producción para desarrollo, pruebas u otros fines.

Puede crear más de un clon desde el mismo clúster de base de datos de Amazon DocumentDB. También puede crear varios clones desde otro clon.

Tras crear un clon de Amazon DocumentDB, puede configurar las instancias de Amazon DocumentDB de forma diferente a la del clúster de Amazon DocumentDB de origen. Por ejemplo, es posible que no necesite un clon con fines de desarrollo para cumplir con los mismos requisitos de alta disponibilidad que el clúster de base de datos Amazon DocumentDB de producción de origen. En este caso, puede configurar el clon con una única instancia de base de datos de Amazon DocumentDB en lugar de las múltiples instancias de base de datos utilizadas por el clúster de base de datos de Amazon DocumentDB.

Cuando termine de utilizar el clon para realizar pruebas, desarrollo u otros fines, puede eliminarlo.

Limitaciones de la clonación de Amazon DocumentDB

La clonación de Amazon DocumentDB tiene las siguientes limitaciones:

- Puede crear tantos clones como desee, hasta el número máximo de clústeres de base de datos permitido en la Región de AWS. No obstante, después de crear 15 clones, el siguiente es una copia completa. La operación de clonación actúa como una point-in-time recuperación.
- No puede crear un clon en una AWS región diferente del clúster de Amazon DocumentDB de origen.
- No se puede crear un clon desde un clúster de base de datos de Amazon DocumentDB que no tiene instancias de base de datos. Solo se pueden clonar clústeres de base de datos de Amazon DocumentDB que tengan al menos una instancia de base de datos.
- Se puede crear un clon en una nube privada virtual (VPC) diferente de la del clúster de base de datos de Amazon DocumentDB. Si lo hace, las subredes del mismo VPCs deben asignarse a las mismas zonas de disponibilidad.

Cómo funciona la clonación de Amazon DocumentDB

La clonación de Amazon DocumentDB funciona en la capa de almacenamiento de un clúster de Amazon DocumentDB. Utiliza un copy-on-writeprotocolo que es rápido y ahorra espacio en cuanto al soporte duradero subyacente que soporta el volumen de almacenamiento de Amazon DocumentDB. Puede obtener más información sobre volúmenes de clúster de Amazon DocumentDB en Administración de clústeres de Amazon DocumentDB.

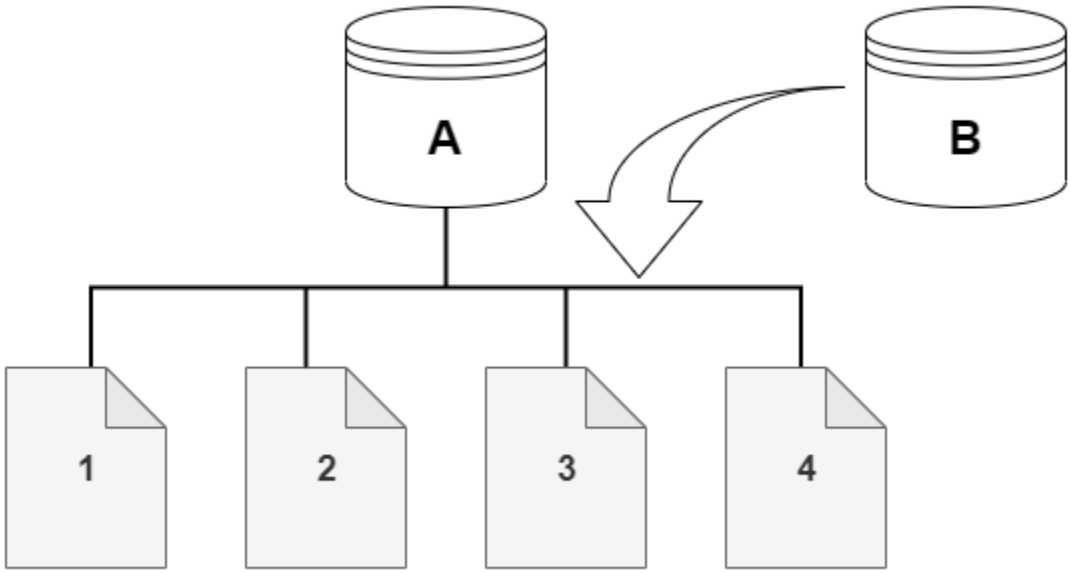
Temas

- Comprensión del protocolo copy-on-write
- Eliminación de un volumen del clúster de origen

Comprensión del protocolo copy-on-write

Un clúster de Amazon DocumentDB almacena datos en páginas en el volumen de almacenamiento de Amazon DocumentDB subyacente.

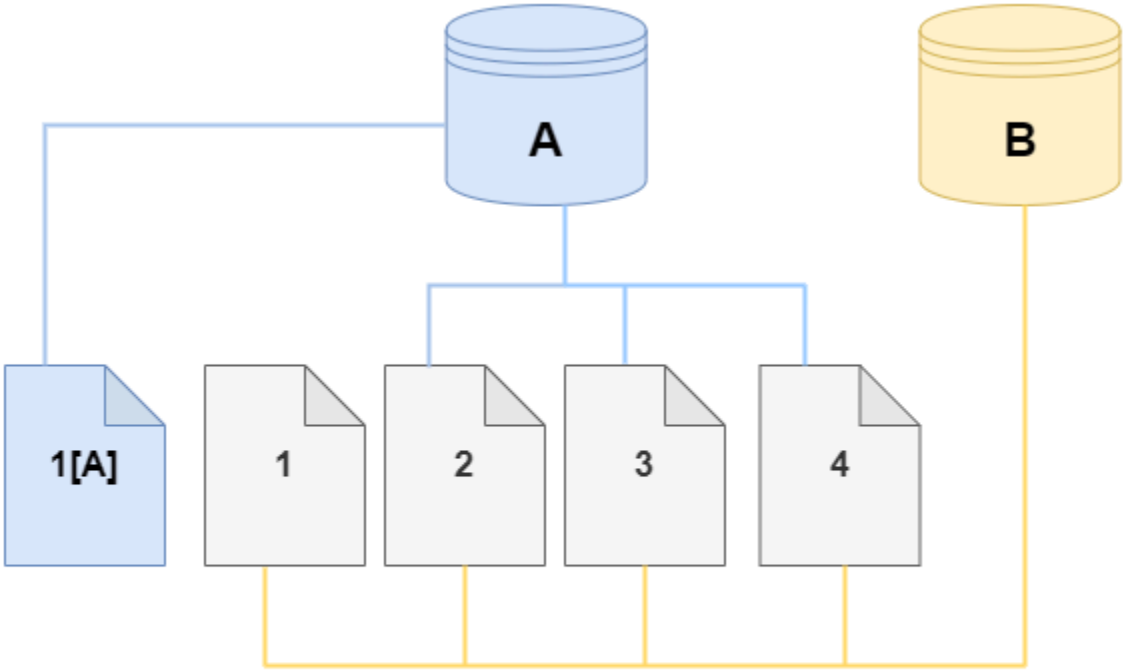
Por ejemplo, en el siguiente diagrama puede encontrar un clúster de base de datos de Amazon DocumentDB (A) que tiene cuatro páginas de datos, 1, 2, 3 y 4. Imagine que un clon, B, se crea desde del clúster de base de datos de Amazon DocumentDB. Cuando se crea el clon, no se copian datos. Más bien, el clon apunta al mismo conjunto de páginas que el clúster de base de datos de Amazon DocumentDB de origen.



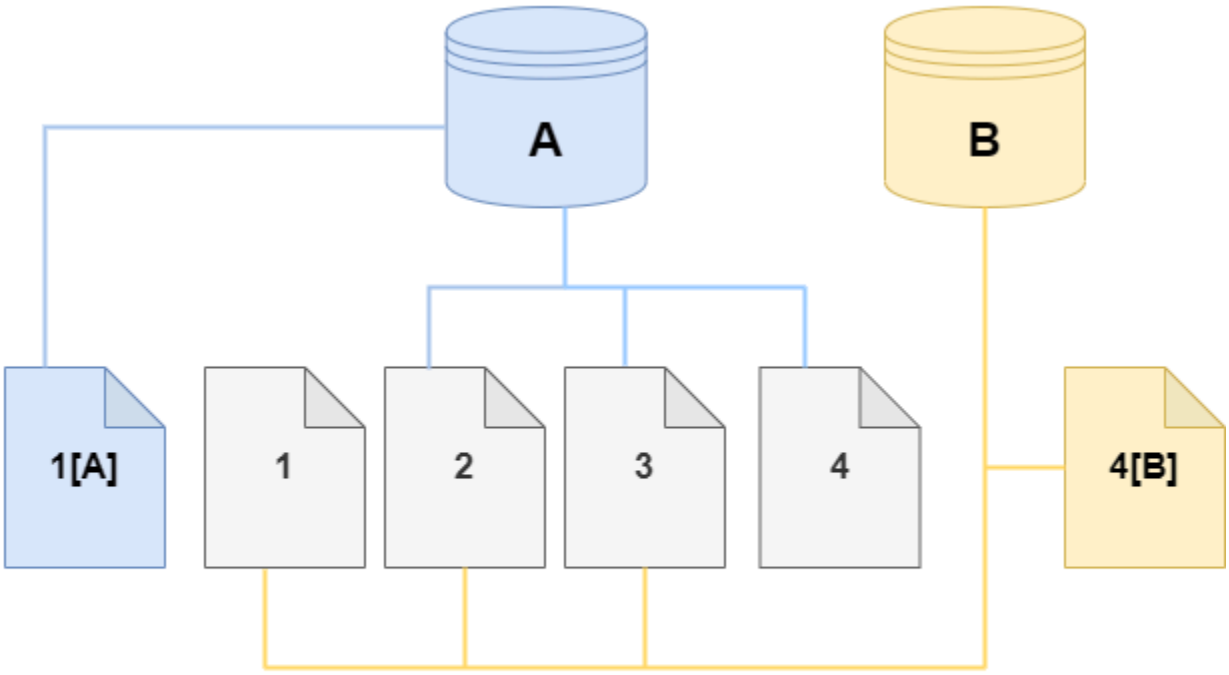
Cuando se crea el clon, generalmente no se necesita almacenamiento adicional. El copy-on-write protocolo utiliza el mismo segmento en el medio de almacenamiento físico que el segmento de origen. Solo se requiere almacenamiento adicional si la capacidad del segmento de origen no es suficiente para todo el segmento de clones. Si ese es el caso, el segmento de origen se copia en otro dispositivo físico.

En los siguientes diagramas, puede encontrar un ejemplo del copy-on-write protocolo en acción que utiliza el mismo clúster A y su clon, B, como se muestra anteriormente. Supongamos que realiza un cambio en su clúster de base de datos de Amazon DocumentDB (A) que da lugar a un cambio en los datos almacenados en la página 1. En lugar de escribir en la página original 1, Amazon DocumentDB

crea una nueva página 1 [A]. El volumen del clúster de base de datos de Amazon DocumentDB para el clúster (A) ahora apunta a la página 1 [A], 2, 3 y 4, mientras que el clon (B) sigue haciendo referencia a las páginas originales.



En el clon, se realiza un cambio en la página 4 del volumen de almacenamiento. En lugar de escribir en la página original 4, Amazon DocumentDB crea una nueva página 4 [B]. El clon ahora apunta a las páginas 1, 2, 3 y a la página 4 [B], mientras que el clúster (A) continúa apuntando a 1 [A], 2, 3 y 4.



A medida que se producen más cambios a lo largo del tiempo en el clon y el volumen del clúster de base de datos de Amazon DocumentDB de origen, necesitará cada vez más almacenamiento para capturar y almacenar los cambios.

Eliminación de un volumen del clúster de origen

Cuando elimina un volumen del clúster de origen que tiene uno o más clones asociados, los clones no se ven afectados. Los clones siguen apuntando a las páginas que antes pertenecían al volumen del clúster de origen.

Creación de un clon de Amazon DocumentDB

Puede crear un clon en la misma AWS cuenta que el clúster de Amazon DocumentDB de origen. Para ello, puede utilizar los procedimientos siguientes Consola de administración de AWS o AWS CLI los siguientes.

Al utilizar la clonación de Amazon DocumentDB, puede crear un clon de clúster de Amazon DocumentDB aprovisionado a partir de un clúster de Amazon DocumentDB aprovisionado.

Using the Consola de administración de AWS

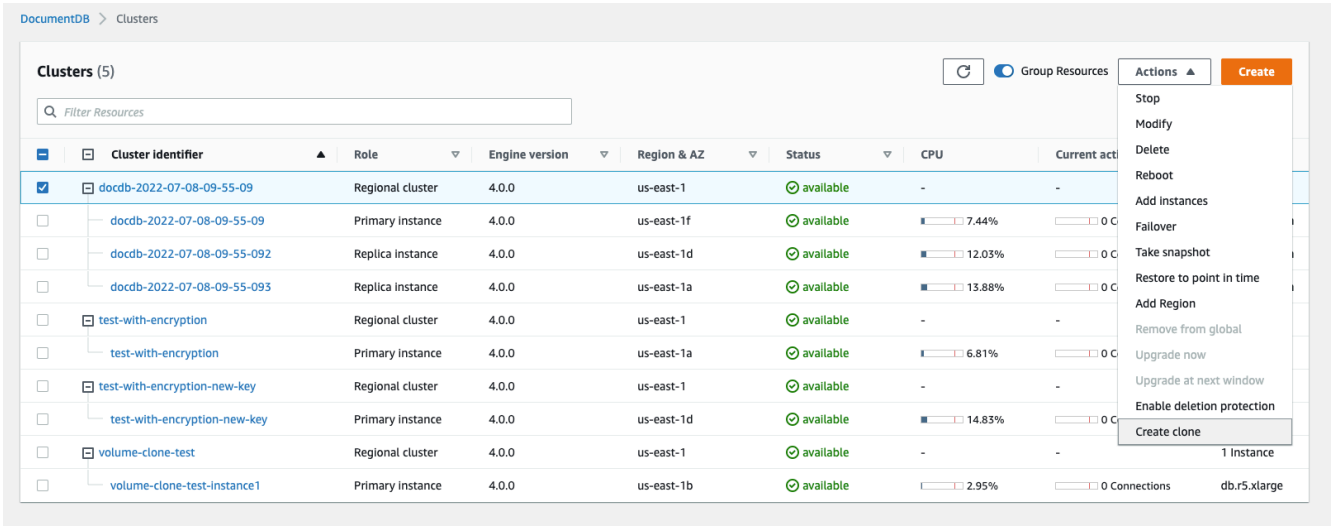
El siguiente procedimiento describe cómo clonar un clúster de Amazon DocumentDB usando la Consola de administración de AWS.

Crear un clon con los Consola de administración de AWS resultados de un clúster de Amazon DocumentDB con una instancia de Amazon DocumentDB.

Estas instrucciones se aplican a los clústeres de bases de datos que pertenecen a la misma AWS cuenta que está creando el clon. El clúster de base de datos debe ser propiedad de la misma AWS cuenta, ya que Amazon DocumentDB no admite la clonación entre cuentas.

Para crear un clon de un clúster de base de datos propiedad de su AWS cuenta mediante el Consola de administración de AWS

1. Inicie sesión en y abra la Consola de administración de AWS consola de Amazon DocumentDB en https://console.aws.amazon.com /docdb.
2. En el panel de navegación, seleccione Clusters (Clústeres).
3. Elija su clúster de base de datos de Amazon DocumentDB de la lista y para Acciones, elija Crear clon.

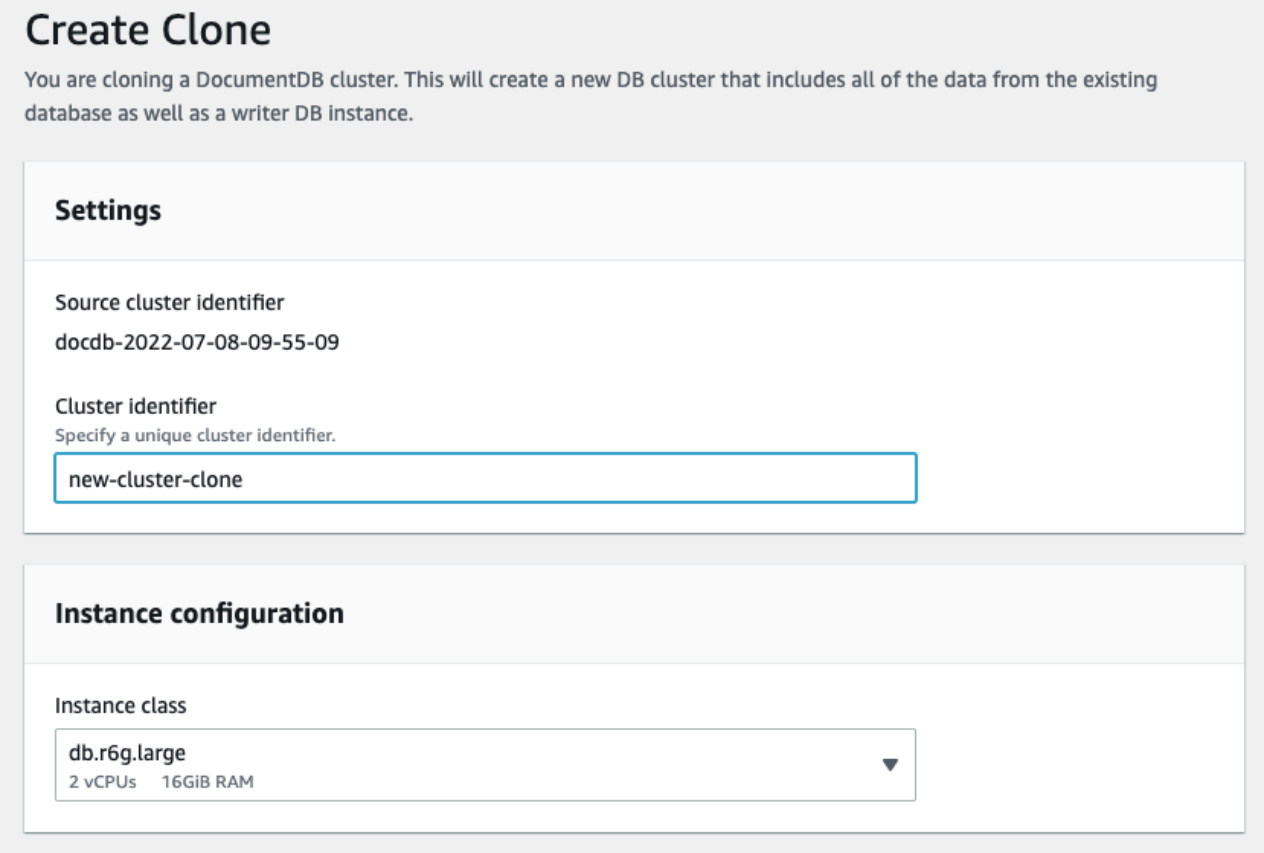


Se abre la página Crear clon, donde puede configurar un Identificador de clúster y una Clase de instancia, y otras opciones para el clon del clúster de Amazon DocumentDB.

4. En la sección Settings, realice lo siguiente:

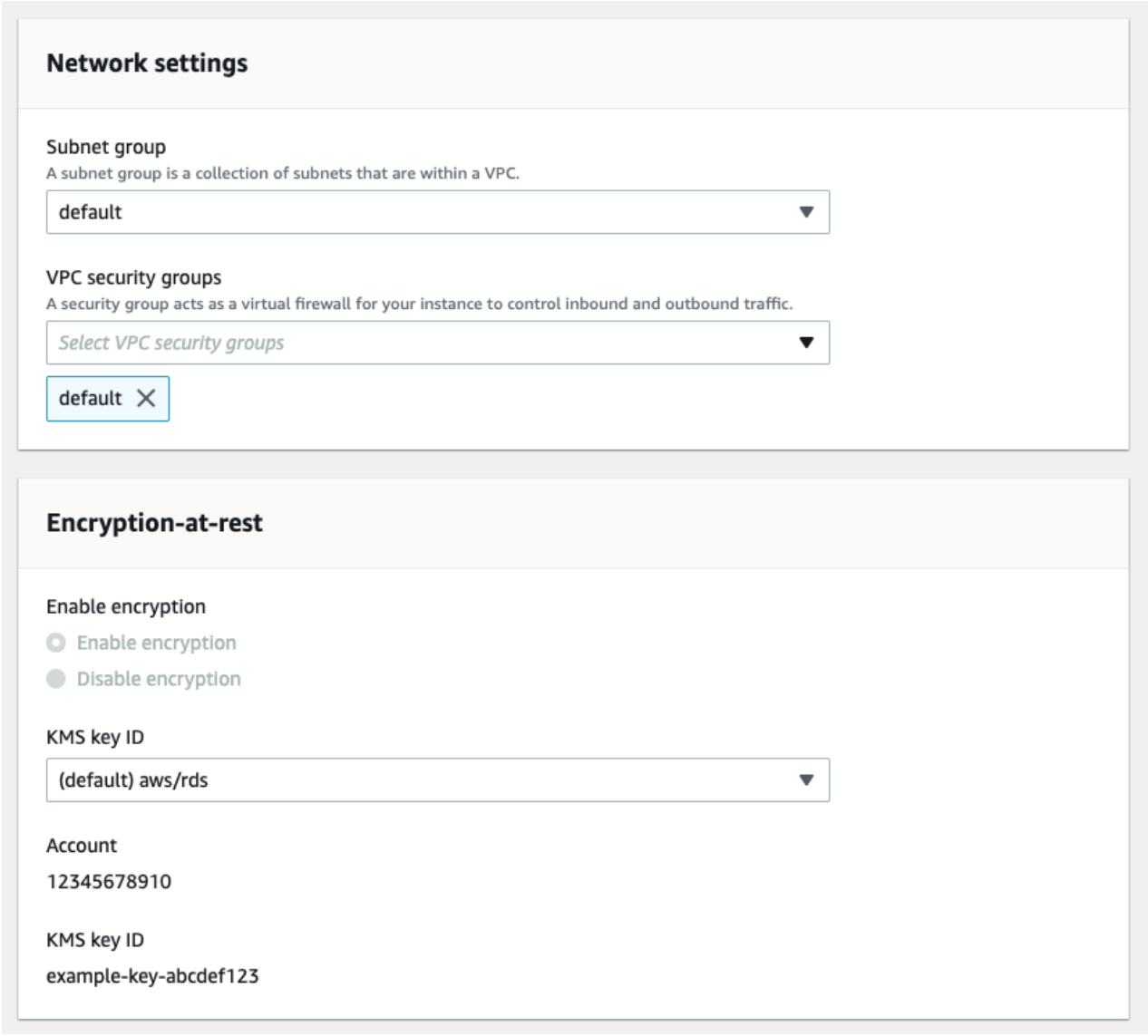
   a. Para el identificador de clúster de base de datos, ingrese el nombre que desea dar a su clúster de base de datos de Amazon DocumentDB clonado.

b. Para la Configuración de instancias, seleccione una Clase de instancia adecuada para su clúster clonado de Amazon DocumentDB.

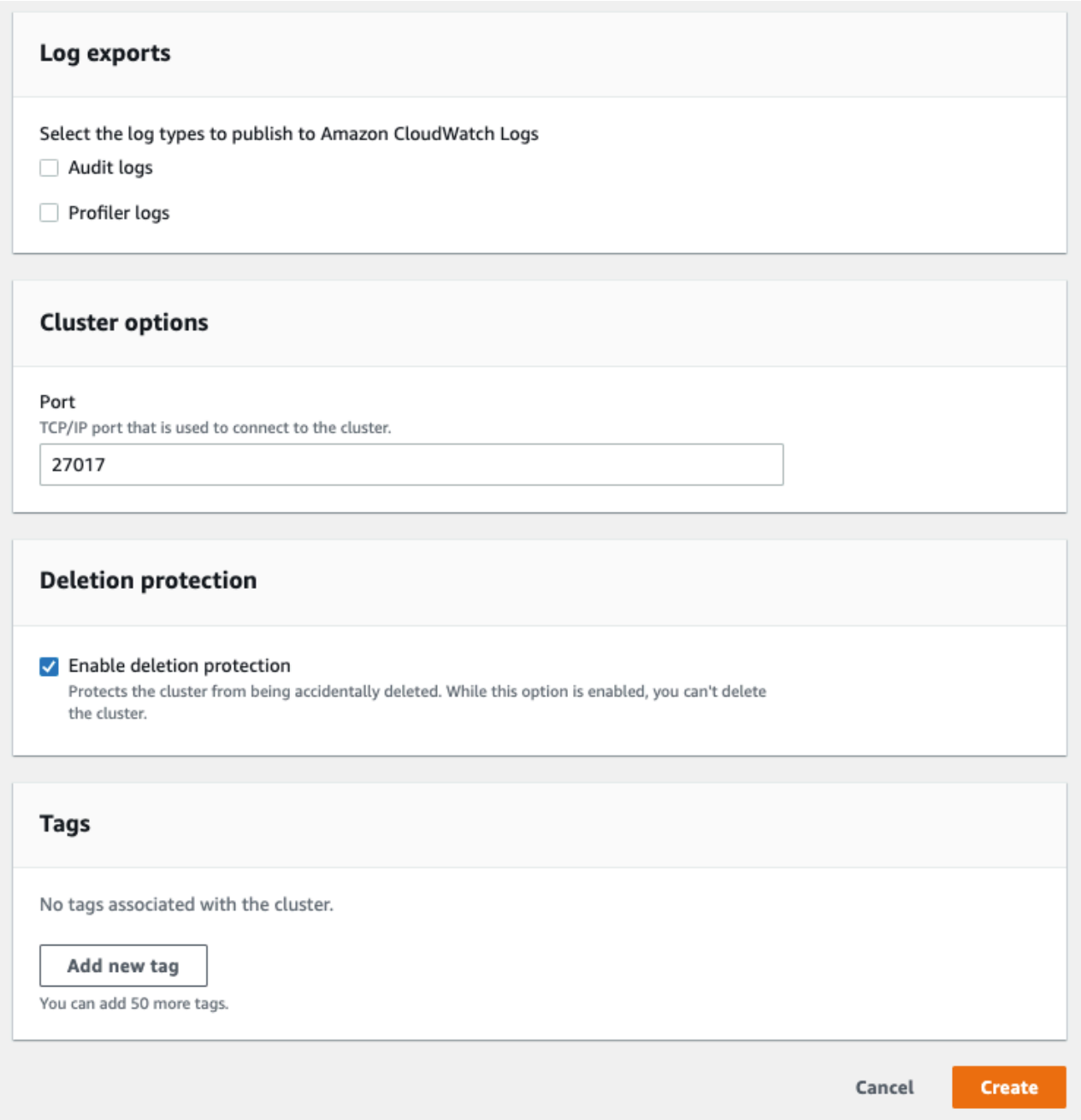


c. En la Configuración de red, elija un Grupo de subredes para su caso de uso y los grupos de seguridad de VPC asociados.

d. En el caso de E ncryption-at-rest, si el clúster de origen (el clúster que se está clonando) tiene el cifrado activado, el clúster clonado también debe tener el cifrado activado. Si se da este escenario, las opciones de Habilitar el cifrado aparecen atenuadas (deshabilitadas), pero con la opción Habilitar el cifrado seleccionada. Por el contrario, si el clúster de origen no tiene el cifrado habilitado, están disponibles las opciones de Habilitar el cifrado y puede elegir habilitar o deshabilitar el cifrado.



e. Complete la nueva configuración del clon del clúster seleccionando el tipo de registros que desea exportar (opcional), introduciendo un puerto específico utilizado para conectarse al clúster y habilitando la protección contra la eliminación accidental del clúster (esta opción está habilitada de forma predeterminada).



f. Termine de ingresar todos los ajustes para su clon de clúster de base de datos de Amazon DocumentDB. Para obtener más información sobre la configuración del clúster y de la instancia de base de datos de Amazon DocumentDB, consulte Administración de clústeres de Amazon DocumentDB.

5. Seleccione Crear clon para lanzar el clon de Amazon DocumentDB del clúster de Amazon DocumentDB que haya elegido.

Cuando se crea el clon, aparece junto con los otros clústeres de base de datos de Amazon DocumentDB en la sección Bases de datos de la consola y muestra su estado actual. Su clon está listo para utilizar cuando su estado es Available (Disponible).

Using the AWS CLI

El uso de AWS CLI para clonar el clúster de Amazon DocumentDB implica un par de pasos.

El `restore-db-cluster-to-point-in-time` AWS CLI comando que utiliza da como resultado un clúster de Amazon DocumentDB vacío con 0 instancias de Amazon DocumentDB. Es decir, el comando restaura solo el clúster de base de datos de Amazon DocumentDB, no las instancias de base de datos de dicho clúster. Lo hace por separado después de que el clon está disponible. Los dos pasos en el proceso son los siguientes:

1. Cree el clon mediante el comando restore-db-cluster-to- point-in-time CLI. Los parámetros que utiliza con este comando controlan el tipo de capacidad y otros detalles del clúster vacío (clon) de base de datos de Amazon DocumentDB que se está creando.
2. Cree la instancia de Amazon DocumentDB para el clon mediante el comando create-db-instanceCLI para volver a crear la instancia de Amazon DocumentDB en el clúster de Amazon DocumentDB restaurado.

Los comandos siguientes asumen que AWS CLI está configurado con su AWS región como predeterminada. Este enfoque le ahorra pasar el nombre de `--region` en cada uno de los comandos. Para obtener más información, consulte Configuración de la AWS CLI. También puede especificar la `--region` en cada uno de los comandos de la CLI que siguen.

Creación del clon

Los parámetros específicos que se pasan al comando `restore-db-cluster-to-point-in-time` de la CLI varían. Lo que pase dependerá del tipo de clon que desea crear.

Utilice el siguiente procedimiento para crear un clon de Amazon DocumentDB aprovisionado a partir de un clúster de Amazon DocumentDB aprovisionado.

Creación de un clon del mismo modo de motor que el clúster de base de datos de Amazon DocumentDB de origen

- Utilice el comando `restore-db-cluster-to-point-in-time` de la CLI y especifique los valores para los siguientes parámetros:

- `--db-cluster-identifier`: elija un nombre significativo para su clon. Se asigna un nombre al clon cuando se utiliza el comando restore-db-cluster-to- point-in-time CLI.
- `--restore-type`: utilice `copy-on-write` para crear un clon del clúster de base de datos de origen. Sin este parámetro, `restore-db-cluster-to-point-in-time` restaura el clúster de base de datos de Amazon DocumentDB en lugar de crear un clon. El valor predeterminado para `restore-type` es `full-copy`.
- `--source-db-cluster-identifier`: utilice el nombre del clúster de base de datos de Amazon DocumentDB de origen que desea clonar.
- `--use-latest-restorable-time`: este valor apunta a los datos de volumen restaurables más recientes para el clon. Este parámetro es obligatorio para `restore-type copy-on-write`, pero no se puede utilizar `restore-to-time parameter` con él.

El siguiente ejemplo crea un clon del clúster de denominado `my-clone` desde un clúster denominado `my-source-cluster`.

Para Linux, macOS o Unix:

```
aws docdb restore-db-cluster-to-point-in-time \
    --source-db-cluster-identifier my-source-cluster \
    --db-cluster-identifier my-clone \
    --restore-type copy-on-write \
    --use-latest-restorable-time
```

Para Windows:

```
aws docdb restore-db-cluster-to-point-in-time ^
    --source-db-cluster-identifier my-source-cluster ^
    --db-cluster-identifier my-clone ^
    --restore-type copy-on-write ^
    --use-latest-restorable-time
```

El comando devuelve el objeto JSON que contiene detalles del clon. Compruebe que su clúster de base de datos clonado está disponible antes de intentar crear la instancia de base de datos para su clon. Para obtener más información, consulte Comprobar el estado y obtener detalles del clon a continuación:

Comprobación del estado y obtención de detalles del clon

Puede utilizar el siguiente comando para verificar el estado del clúster de base de datos vacío recién creado.

```
$ aws docdb describe-db-clusters --db-cluster-identifier my-clone --query '*[].
[Status]' --output text
```

O bien, puede obtener el estado y los demás valores que necesita para crear la instancia de base de datos para el clon mediante la siguiente AWS CLI consulta:

Para Linux, macOS o Unix:

```
aws docdb describe-db-clusters --db-cluster-identifier my-clone \
  --query '*[].{Status:Status,Engine:Engine,EngineVersion:EngineVersion}'
```

Para Windows:

```
aws docdb describe-db-clusters --db-cluster-identifier my-clone ^
  --query "*[].{Status:Status,Engine:Engine,EngineVersion:EngineVersion}"
```

Esta consulta devuelve un resultado similar al siguiente:

```
[
  {
        "Status": "available",
        "Engine": "docdb",
        "EngineVersion": "4.0.0",
    }
]
```

Creación de la instancia de Amazon DocumentDB para su clon

Utilice el comando create-db-instanceCLI para crear la instancia de base de datos para el clon.

El parámetro `--db-instance-class` se utiliza sólo para clústeres de base de datos aprovisionados de Amazon DocumentDB.

Para Linux, macOS o Unix:

```
aws docdb create-db-instance \
    --db-instance-identifier my-new-db \
    --db-cluster-identifier my-clone \
    --db-instance-class  db.r5.4xlarge \
```

```
    --engine docdb
```

Para Windows:

```
aws docdb create-db-instance ^
    --db-instance-identifier my-new-db ^
    --db-cluster-identifier my-clone ^
    --db-instance-class  db.r5.4xlarge ^
    --engine docdb
```

Parámetros para utilizar durante la clonación

En la siguiente tabla se resumen los diversos parámetros utilizados con `restore-db-cluster-to-point-in-time` para clonar clústeres de base de datos de Amazon DocumentDB.

Parámetro	Description (Descripción)
--source-db-cluster-identifier	Utilice el nombre del clúster de base de datos de Amazon DocumentDB de origen que desea clonar.
--db-cluster-identifier	Elija un nombre significativo para su clon. Asigne un nombre a su clon con el comando `restore-db-cluster-to-point-in-time`. A continuación, pase este nombre al comando `create-db-instance` .
—restore-type	Especifique `copy-on-write` como el `--restore-type` para crear un clon del clúster de base de datos de origen en lugar de restaurar el clúster de base de datos de Amazon DocumentDB de origen.
--use-latest-restorable-time	Este valor apunta a los datos de volumen restaurables más recientes para el clon.

Información general de la tolerancia a errores de clúster de Amazon DocumentDB

Los clústeres de Amazon DocumentDB ofrecen tolerancia a errores por diseño. El volumen de cada clúster abarca varias zonas de disponibilidad en una sola Región de AWS, y cada zona de

disponibilidad contiene una copia de los datos del volumen del clúster. Esta funcionalidad significa que el clúster puede tolerar un error de una zona de disponibilidad sin perder datos y con tan solo una interrupción breve del servicio.

Si se produce un error en la instancia principal de un clúster de base de datos, Amazon DocumentDB conmuta automáticamente a una nueva instancia principal de una de las dos formas siguientes:

- Promocionando una réplica de Amazon DocumentDB existente a la nueva instancia principal elegida en función de la configuración del nivel de promoción de cada réplica y, a continuación, creando una que sustituya a la anterior principal. Una conmutación por error a la instancia de réplica suele tardar menos de 30 segundos. Las operaciones de lectura y escritura pueden sufrir breves interrupciones durante este período. Para aumentar la disponibilidad de su clúster de base de datos, es recomendable que cree al menos una o varias réplicas de Amazon DocumentDB en dos o más zonas de disponibilidad diferentes.
- Creando una nueva instancia principal. Esto solo ocurre si no tiene una instancia de réplica en el clúster y puede tardar unos minutos en completarse.

Si el clúster tiene una o varias réplicas de Amazon DocumentDB, se promueve una réplica de Amazon DocumentDB a instancia principal durante un evento de error. Un evento de error provoca una interrupción breve durante la cual las operaciones de lectura y escritura generan errores con una excepción. Sin embargo, el servicio se suele restaurar en menos de 120 segundos y, en muchos casos, en menos de 60 segundos. Para aumentar la disponibilidad de su clúster de base de datos, es recomendable que cree al menos una o varias réplicas de Amazon DocumentDB en dos o más zonas de disponibilidad diferentes.

Puede personalizar el orden en que se promueven las réplicas de Amazon DocumentDB a instancia principal tras un error mediante la asignación de una prioridad a cada réplica. Las prioridades van desde 0 para la prioridad más alta hasta 15 para la más baja. Si la instancia principal experimenta un error, la réplica de Amazon DocumentDB que tenga la máxima prioridad pasará a ser la instancia principal. Puede modificar la prioridad de una réplica de Amazon DocumentDB en cualquier momento. Al modificar la prioridad, no se activa una conmutación por error. Puede usar la operación `modify-db-instance` con el parámetro `--promotion-tier`. Para obtener más información acerca de cómo personalizar la prioridad de conmutación por error de una instancia, consulte Conmutación por error a Amazon DocumentDB.

Puede haber más de una réplica de Amazon DocumentDB con la misma prioridad, lo que genera niveles de promoción. Si dos o más réplicas de Amazon DocumentDB comparten la misma prioridad, pasará a ser la instancia principal la réplica que tiene un tamaño mayor. Si dos o más réplicas

de Amazon DocumentDB tienen la misma prioridad y el mismo tamaño, se promueve una réplica arbitraria del mismo nivel de promoción.

Si el clúster no contiene ninguna réplica de Amazon DocumentDB, la instancia principal se vuelve a crear durante un evento de error. Un evento de error provoca una interrupción durante la cual las operaciones de lectura y escritura generan errores con una excepción. El servicio se restaura cuando se crea la nueva instancia principal, un proceso que normalmente dura menos de 10 minutos. Promover una réplica de Amazon DocumentDB a instancia principal es mucho más rápido que crear una nueva instancia principal.

Administración de instancias de Amazon DocumentDB

Los siguientes temas proporcionan información que le ayudarán a administrar sus instancias de Amazon DocumentDB. Incluyen detalles sobre las clases y los estados de instancias, y cómo crear, eliminar y modificar una instancia.

Temas

- Determinación del estado de una instancia
- Ciclo de vida de instancia de Amazon DocumentDB
- Administración de clases de instancias
- Instancias respaldadas por NVMe

Determinación del estado de una instancia

Para ver los estados válidos de las instancias, su significado y saber cómo determinar el estado de las instancias, consulte Supervisión del estado de un clúster de Amazon DocumentDB.

Ciclo de vida de instancia de Amazon DocumentDB

El ciclo de vida de una instancia Amazon DocumentDB comprende su creación, modificación, mantenimiento y actualización, ejecución de copias de seguridad y restauraciones, reinicio, actualización y eliminación. En esta sección se proporciona información sobre cómo realizar estos procesos.

Temas

- Agregación de una instancia de Amazon DocumentDB a un clúster
- Descripción de las instancias de Amazon DocumentDB

- Modificación de una instancia de base de datos de Amazon DocumentDB
- Reinicio de la instancia de Amazon DocumentDB
- Eliminación de una instancia de Amazon DocumentDB

Puede crear una nueva instancia de Amazon DocumentDB utilizando la Consola de administración de AWS o la AWS CLI. Para añadir una instancia a un clúster, el clúster debe tener un estado disponible. No puede añadir una instancia a un clúster que está detenido. Si el clúster está detenido, inicie primero el clúster, espere a que el clúster esté disponible y, a continuación, añada una instancia. Para obtener más información, consulte Detención e inicio de un clúster de bases de datos de Amazon DocumentDB.

> **Note**
>
> Si crea un clúster de Amazon DocumentDB mediante la consola, se crea automáticamente una instancia al mismo tiempo. Si desea crear instancias adicionales, utilice uno de los siguientes procedimientos.

Agregación de una instancia de Amazon DocumentDB a un clúster

Using the Consola de administración de AWS

El siguiente procedimiento permite crear una instancia de su clúster mediante la consola de Amazon DocumentDB.

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon DocumentDB en https://console.aws.amazon.com/docdb.
2. En el panel de navegación, seleccione Clusters (Clústeres).

   > **Tip**
   >
   > Si no ve el panel de navegación del lado izquierdo de la pantalla, seleccione el icono de menú
   > (≡)
   > en la esquina superior izquierda de la página.

3. Para elegir el clúster al que desea añadir una instancia, seleccione el botón situado a la izquierda del nombre del clúster.

4. Elija Actions (Acciones) y después Add instances (Añadir instancias).
5. En la página Add instance to (Añadir instancia a)<cluster-name>, repita los pasos que se describen a continuación para cada instancia que desee añadir al clúster. Puede tener un máximo de 15.

   a. Instance identifier: puede escribir un identificador único para esta instancia o permitir que Amazon DocumentDB proporcione el identificador de la instancia basándose en el identificador del clúster.

      Restricciones en cuanto a la nomenclatura de las instancias:

      - Debe tener [1-63] letras, números o guiones.
      - El primer carácter debe ser una letra.
      - No puede terminar por un guion ni contener dos guiones consecutivos.
      - Debe ser único para todas las instancias de Amazon RDS, Neptune y Amazon DocumentDB por Cuenta de AWS y por región.

   b. Clase de instancia: en la lista desplegable, elija el tipo de instancia que desea para esta instancia.

   c. Capa de promoción: en la lista, elija la capa de promoción de la instancia, o bien elija Sin preferencia para permitir que Amazon DocumentDB establezca la capa de promoción de la instancia. Un número menor indica una mayor prioridad. Para obtener más información, consulte Control del destino de la conmutación por error.

   d. Para añadir más instancias, elija Add additional instances (Agregar instancias adicionales) y repita los pasos a, b y c.

6. Finalizar la operación.

   - Para añadir las instancias a su clúster, seleccione Create (Crear).
   - Para cancelar la operación, elija Cancel (Cancelar).

La creación de una instancia puede tardar varios minutos. Puede usar la consola o la AWS CLI para ver el estado de la instancia. Para obtener más información, consulte Monitorización del estado de una instancia.

Using the AWS CLI

Utilice la operación `create-db-instance` de la AWS CLI con los siguientes parámetros para crear la instancia principal para el clúster.

- **`--db-instance-class`**: obligatorio. La capacidad de memoria e informática de la instancia (por ejemplo,)., `db.m4.large`. No todas las clases de instancia están disponibles en todas las Regiones de AWS.
- **`--db-instance-identifier`**: obligatorio. Una cadena que identifica la instancia.

  Restricciones en cuanto a la nomenclatura de las instancias:

  - Debe tener [1-63] letras, números o guiones.
  - El primer carácter debe ser una letra.
  - No puede terminar por un guion ni contener dos guiones consecutivos.
  - Debe ser único para todas las instancias de Amazon RDS, Neptune y Amazon DocumentDB por Cuenta de AWS y por región.
- **`--engine`**: obligatorio. Debe ser `docdb`.
- **`--availability-zone`**: opcional. La zona de disponibilidad en la que desea crear esta instancia. Use este parámetro para colocar sus instancias en diferentes zonas de disponibilidad con el fin de aumentar la tolerancia a errores. Para obtener más información, consulte Alta disponibilidad y replicación de Amazon DocumentDB.
- **`--promotion-tier`**: opcional. El nivel de prioridad de conmutación por error de esta instancia. Debe ser un número comprendido entre 0 y 15; un número menor indica una mayor prioridad. Para obtener más información, consulte Control del destino de la conmutación por error.

1. En primer lugar, determine en qué zonas de disponibilidad puede crear la instancia.

   Si desea especificar la zona de disponibilidad, antes de crear la instancia, ejecute el siguiente comando para determinar en qué zonas de disponibilidad están disponibles para el clúster de Amazon DocumentDB.

   Para Linux, macOS o Unix:

   ```
   aws docdb describe-db-clusters \
         --query 'DBClusters[*].[DBClusterIdentifier,AvailabilityZones[*]]'
   ```

   Para Windows:

   ```
   aws docdb describe-db-clusters ^
         --query 'DBClusters[*].[DBClusterIdentifier,AvailabilityZones[*]]'
   ```

La salida de esta operación será similar a lo que se indica a continuación.

```
[
    [
        "sample-cluster",
        [
            "us-east-1c",
            "us-east-1b",
            "us-east-1a"
        ]
    ]
]
```

2. En segundo lugar, determine qué clases de instancias puede crear en su región.

   Para determinar qué clases de instancias tiene a su disposición en su región, ejecute el siguiente comando. En el resultado, elija una clase de instancia para la instancia que desea agregar al clúster de Amazon DocumentDB.

   Para Linux, macOS o Unix:

```
aws docdb describe-orderable-db-instance-options \
        --engine docdb \
        --query 'OrderableDBInstanceOptions[*].DBInstanceClass'
```

   Para Windows:

```
aws docdb describe-orderable-db-instance-options ^
        --engine docdb ^
        --query 'OrderableDBInstanceOptions[*].DBInstanceClass'
```

   La salida de esta operación será similar a lo que se indica a continuación.

```
[
    "db.r5.16xlarge",
    "db.r5.2xlarge",
    "db.r5.4xlarge",
    "db.r5.8xlarge",
    "db.r5.large",
    "db.r5.xlarge"
```

```
]
```

3. Agregar una instancia a su clúster de Amazon DocumentDB.

   Para agregar una instancia al clúster de Amazon DocumentDB, ejecute el siguiente comando.

   Para Linux, macOS o Unix:

```
aws docdb create-db-instance \
       --db-cluster-identifier sample-cluster \
       --db-instance-identifier sample-instance-2 \
       --availability-zone us-east-1b \
       --promotion-tier 2 \
       --db-instance-class db.r5.xlarge \
       --engine docdb
```

   Para Windows:

```
aws docdb create-db-instance ^
       --db-cluster-identifier sample-cluster ^
       --db-instance-identifier sample-instance-2 ^
       --availability-zone us-east-1b ^
       --promotion-tier 2 ^
       --db-instance-class db.r5.xlarge ^
       --engine docdb
```

   La salida de esta operación será similar a lo que se indica a continuación.

```
{
    "DBInstance": {
        "DBInstanceIdentifier": "sample-instance-2",
        "DBInstanceClass": "db.r5.xlarge",
        "Engine": "docdb",
        "DBInstanceStatus": "creating",
        "PreferredBackupWindow": "02:00-02:30",
        "BackupRetentionPeriod": 1,
        "VpcSecurityGroups": [
            {
                "VpcSecurityGroupId": "sg-abcd0123",
                "Status": "active"
            }
        ],
```

```
        "AvailabilityZone": "us-east-1b",
        "DBSubnetGroup": {
            "DBSubnetGroupName": "default",
            "DBSubnetGroupDescription": "default",
            "VpcId": "vpc-6242c31a",
            "SubnetGroupStatus": "Complete",
            "Subnets": [
                {
                    "SubnetIdentifier": "subnet-abcd0123",
                    "SubnetAvailabilityZone": {
                        "Name": "us-west-2a"
                    },
                    "SubnetStatus": "Active"
                },
                {
                    "SubnetIdentifier": "subnet-wxyz0123",
                    "SubnetAvailabilityZone": {
                        "Name": "us-west-2b"
                    },
                    "SubnetStatus": "Active"
                }
            ]
        },
        "PreferredMaintenanceWindow": "sun:11:35-sun:12:05",
        "PendingModifiedValues": {},
        "EngineVersion": "3.6.0",
        "AutoMinorVersionUpgrade": true,
        "PubliclyAccessible": false,
        "DBClusterIdentifier": "sample-cluster",
        "StorageEncrypted": true,
        "KmsKeyId": "arn:aws:kms:us-east-1:<accountID>:key/sample-key",
        "DbiResourceId": "db-ABCDEFGHIJKLMNOPQRSTUVWXYZ",
        "CACertificateIdentifier": "rds-ca-2019",
        "PromotionTier": 2,
        "DBInstanceArn": "arn:aws:rds:us-east-1:<accountID>:db:sample-instance-2"
    }
}
```

La creación de la instancia puede tardar varios minutos. Puede usar la consola o la AWS CLI para ver el estado de la instancia. Para obtener más información, consulte Supervisión del estado de un clúster de Amazon DocumentDB.

Descripción de las instancias de Amazon DocumentDB

Puede utilizar la Consola de administración de Amazon DocumentDB o la AWS CLI para ver detalles como puntos de conexión, grupos de seguridad VPC, entidad de certificación y grupos de parámetros relacionados con las instancias de Amazon DocumentDB.

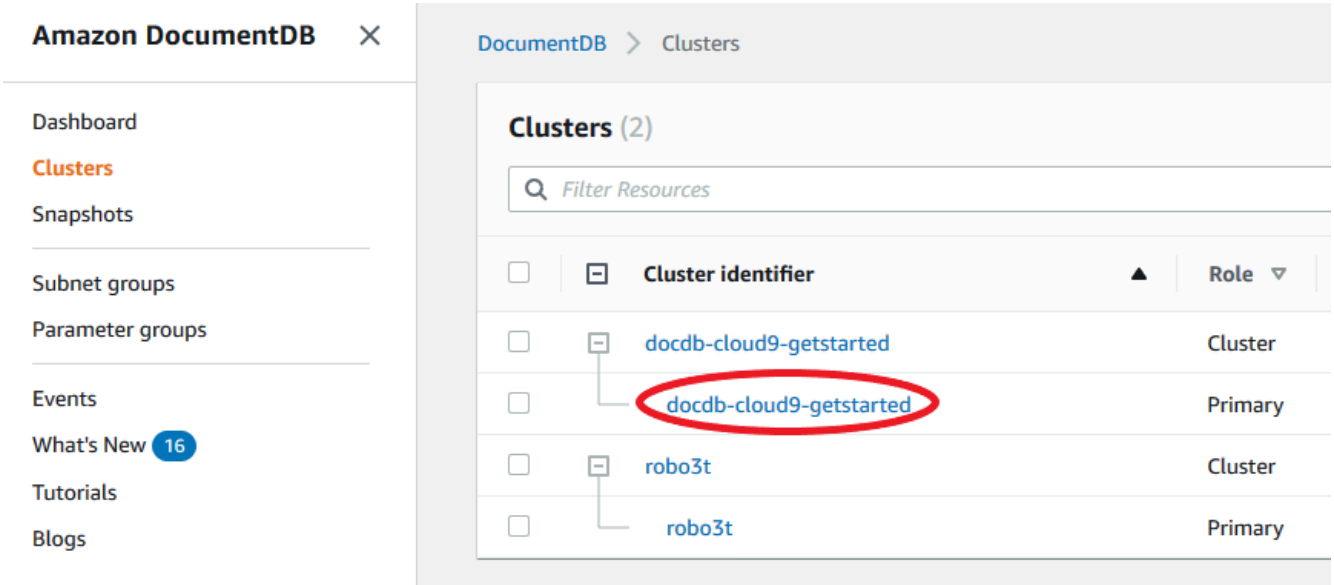
Using the Consola de administración de AWS

Para ver los detalles de las instancias mediante la Consola de administración de AWS, siga los pasos que se indican a continuación.

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon DocumentDB en https://console.aws.amazon.com/docdb.
2. En el panel de navegación, seleccione Clusters (Clústeres).

> **Tip**
>
> Si no ve el panel de navegación del lado izquierdo de la pantalla, seleccione el icono de menú
> (≡)
> en la esquina superior izquierda de la página.

3. En el cuadro de navegación de clústeres, verá la columna Identificador del clúster. Las instancias se muestran en clústeres, de forma similar a la siguiente captura de pantalla.



4. En la lista de instancias, elija el nombre de la instancia cuyos detalles desea ver. La información sobre la instancia se organiza en los siguientes grupos:

   - Resumen: información general sobre la instancia, incluida la versión del motor, la clase, el estado y cualquier mantenimiento pendiente.
   - Conectividad y seguridad: la sección Conectar enumera los puntos de conexión para conectarse a esta instancia con el shell de mongo o con una aplicación. La sección Grupos de seguridad muestra los grupos de seguridad asociados a esta instancia y su ID de VPC y descripciones.
   - Configuración: la sección Detalles muestra las configuraciones y el estado de la instancia, incluidos el nombre de recurso de Amazon (ARN), el punto de conexión, el rol, la clase y la entidad de certificación de la instancia. También enumera la seguridad y la configuración de red de la instancia, así como la información de copia de seguridad. La sección Detalles del clúster muestra los detalles del clúster al que pertenece esta instancia. La sección Instancias del clúster muestra todas las instancias que pertenecen al clúster con el rol de cada instancia y el estado del grupo de parámetros del clúster.

     > **Note**
     >
     > Puede modificar el clúster asociado a la instancia seleccionando Modificar junto al encabezado Detalles del clúster. Para obtener más información, consulte Modificación de un clúster de Amazon DocumentDB.

   - Monitoreo: las métricas de los registros de CloudWatch para esta instancia. Para obtener más información, consulte Supervisión de Amazon DocumentDB con CloudWatch.
   - Eventos y etiquetas: la sección de eventos recientes muestra los eventos recientes de esta instancia. Amazon DocumentDB mantiene un registro de los eventos relacionados con los clústeres, las instancias, las instantáneas, los grupos de seguridad y los grupos de parámetros de clúster. Esta información incluye la fecha, la hora y el mensaje asociados a cada evento. La sección Etiquetas muestra las etiquetas asociadas a este clúster. Para obtener más información, consulte Etiquetado de recursos de Amazon DocumentDB.

Using the AWS CLI

Para ver los detalles de las instancias de Amazon DocumentDB mediante la AWS CLI, utilice el comando `describe-db-clusters` como se muestra en los siguientes ejemplos. Para

obtener más información, consulte `DescribeDBInstances` en la Referencia de la API para administración de recursos de Amazon DocumentDB.

> **Note**
>
> Para ciertas características de administración, como la administración del ciclo de vida de clúster y de instancia, Amazon DocumentDB aprovecha la tecnología operativa que se comparte con Amazon RDS. El parámetro de filtro `filterName=engine,Values=docdb` devuelve solo clústeres de Amazon DocumentDB.

1. Enumere todas las instancias de Amazon DocumentDB.

   El código de la AWS CLI siguiente enumera los detalles de todos las instancias de Amazon DocumentDB de una región.

   Para Linux, macOS o Unix:

   ```
   aws docdb describe-db-instances \
       --filter Name=engine,Values=docdb
   ```

   Para Windows:

   ```
   aws docdb describe-db-instances \
       --filter Name=engine,Values=docdb
   ```

2. Enumeración de todos los detalles de una instancia de Amazon DocumentDB especificada

   El siguiente código enumera los detalles de `sample-cluster-instance`. Incluir el parámetro `--db-instance-identifier` con el nombre de una instancia restringe la salida a la información sobre esa instancia en particular.

   Para Linux, macOS o Unix:

   ```
   aws docdb describe-db-instances \
       --db-instance-identifier sample-cluster-instance
   ```

   Para Windows:

```
aws docdb describe-db-instances \
    --db-instance-identifier sample-cluster-instance
```

El resultado de esta operación será similar a lo que se indica a continuación:

```
{
    "DBInstances": [
        {
            "DbiResourceId": "db-BJKKB54PIDV5QFKGVRX5T3S6GM",
            "DBInstanceArn": "arn:aws:rds:us-east-1:012345678901:db:sample-
cluster-instance-00",
            "VpcSecurityGroups": [
                {
                    "VpcSecurityGroupId": "sg-77186e0d",
                    "Status": "active"
                }
            ],
            "DBInstanceClass": "db.r5.large",
            "DBInstanceStatus": "creating",
            "AutoMinorVersionUpgrade": true,
            "PreferredMaintenanceWindow": "fri:09:32-fri:10:02",
            "BackupRetentionPeriod": 1,
            "StorageEncrypted": true,
            "DBClusterIdentifier": "sample-cluster",
            "EngineVersion": "3.6.0",
            "AvailabilityZone": "us-east-1a",
            "Engine": "docdb",
            "PromotionTier": 2,
            "DBInstanceIdentifier": "sample-cluster-instance",
            "PreferredBackupWindow": "00:00-00:30",
            "PubliclyAccessible": false,
            "DBSubnetGroup": {
                "DBSubnetGroupName": "default",
                "Subnets": [
                    {
                        "SubnetIdentifier": "subnet-4e26d263",
                        "SubnetAvailabilityZone": {
                            "Name": "us-east-1a"
                        },
                        "SubnetStatus": "Active"
                    },
                    {
```

```
                        "SubnetIdentifier": "subnet-afc329f4",
                        "SubnetAvailabilityZone": {
                            "Name": "us-east-1c"
                        },
                        "SubnetStatus": "Active"
                    },
                    {
                        "SubnetIdentifier": "subnet-b3806e8f",
                        "SubnetAvailabilityZone": {
                            "Name": "us-east-1e"
                        },
                        "SubnetStatus": "Active"
                    },
                    {
                        "SubnetIdentifier": "subnet-53ab3636",
                        "SubnetAvailabilityZone": {
                            "Name": "us-east-1d"
                        },
                        "SubnetStatus": "Active"
                    },
                    {
                        "SubnetIdentifier": "subnet-991cb8d0",
                        "SubnetAvailabilityZone": {
                            "Name": "us-east-1b"
                        },
                        "SubnetStatus": "Active"
                    },
                    {
                        "SubnetIdentifier": "subnet-29ab1025",
                        "SubnetAvailabilityZone": {
                            "Name": "us-east-1f"
                        },
                        "SubnetStatus": "Active"
                    }
                ],
                "VpcId": "vpc-91280df6",
                "DBSubnetGroupDescription": "default",
                "SubnetGroupStatus": "Complete"
            },
            "PendingModifiedValues": {},
            "KmsKeyId": "arn:aws:kms:us-east-1:012345678901:key/0961325d-
a50b-44d4-b6a0-a177d5ff730b"
        }
    ]
```

```
}
```

Modificación de una instancia de base de datos de Amazon DocumentDB

Puede modificar su instancia de Amazon DocumentDB mediante la Consola de administración de AWS o la AWS CLI. Para modificar una instancia, la instancia debe tener el estado disponible. No puede modificar una instancia detenida. Si el clúster está detenido, inicie primero el clúster, espere a que la instancia esté disponible y, a continuación, realice las modificaciones deseadas. Para obtener más información, consulte Detención e inicio de un clúster de bases de datos de Amazon DocumentDB.

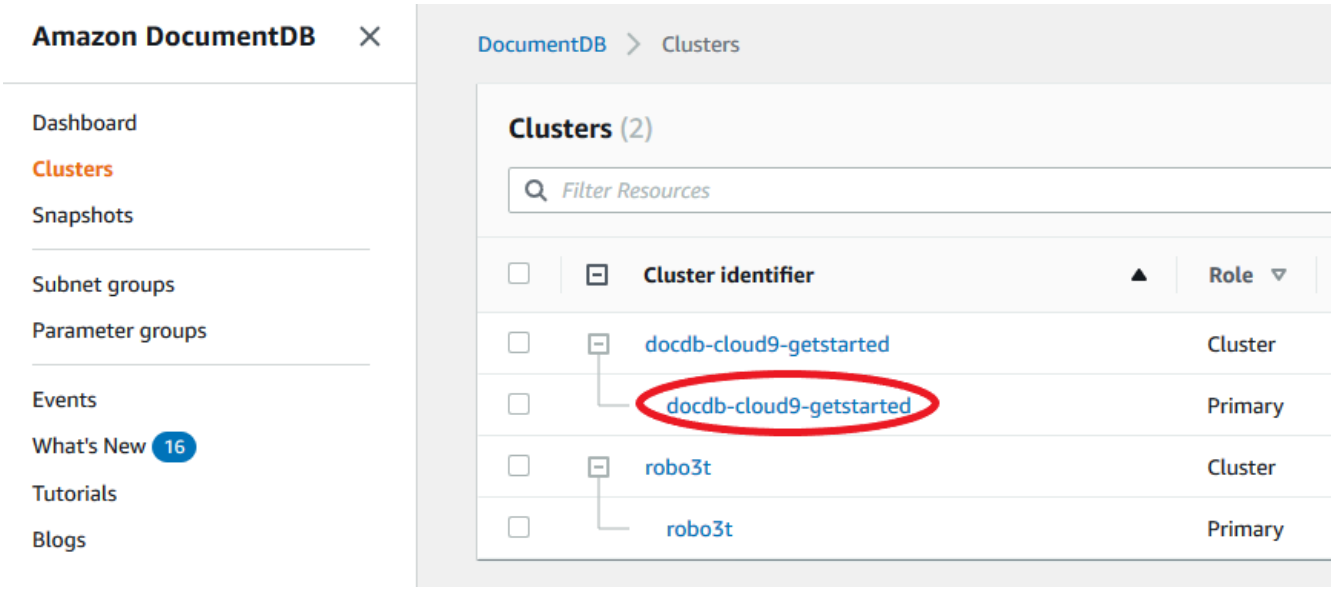
Using the Consola de administración de AWS

Complete los pasos que se indican a continuación para modificar una instancia de Amazon DocumentDB específica mediante la consola.

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon DocumentDB en https://console.aws.amazon.com/docdb.
2. En el panel de navegación, seleccione Clusters (Clústeres).

   > **Tip**
   >
   > Si no ve el panel de navegación del lado izquierdo de la pantalla, seleccione el icono de menú
   > (≡)
   > en la esquina superior izquierda de la página.

3. En el cuadro de navegación de clústeres, verá la columna Identificador del clúster. Las instancias se muestran en clústeres, de forma similar a la siguiente captura de pantalla.



4. Marque la casilla de verificación situada a la izquierda de la instancia que desea modificar.
5. Elija Actions (Acciones) y después Modify (Modificar).
6. En el panel Modificar instancia: <instance-name>, realice los cambios que desee. Puede hacer los siguientes cambios:

   - Especificaciones de instancia: el identificador y la clase de la instancia. Restricciones de nombres del identificador de instancia:
     - Identificador de instancia: escriba un nombre que sea único para todas las instancias pertenecientes a su Cuenta de AWS en la región actual. El identificador de instancia debe contener [1-63] caracteres alfanuméricos o guiones, tener una letra como primer carácter y no puede terminar con un guion ni contener dos guiones consecutivos.
     - Clase de instancia: en el menú desplegable, seleccione una clase de instancia para su instancia de Amazon DocumentDB. Para obtener más información, consulte Administración de clases de instancias.
   - Autoridad de certificación: certificado de servidor para esta instancia. Para obtener más información, consulte Actualización de los certificados TLS de Amazon DocumentDB.
   - Conmutación por error: durante la conmutación por error, la instancia con el nivel de promoción más alto se promoverá a primaria. Para obtener más información, consulte Conmutación por error a Amazon DocumentDB.
   - Mantenimiento : la ventana de mantenimiento en la que se aplican las modificaciones o revisiones pendientes a las instancias del clúster.
7. Cuando haya terminado, elija Continuar para ver un resumen de los cambios.

8. Después de verificar los cambios, puede aplicarlos inmediatamente o durante el siguiente período de mantenimiento en Scheduling of modifications (Programación de modificaciones). Seleccione Modify instance (Modificar instancia) para guardar los cambios. Como alternativa, puede elegir Cancel (Cancelar) para descartar los cambios.

Los cambios pueden tardar unos minutos en aplicarse. Solo puede usar la instancia cuando su estado sea available (disponible). Puede monitorizar el estado de la instancia mediante la consola o la AWS CLI. Para obtener más información, consulte Supervisión del estado de un clúster de Amazon DocumentDB.

Using the AWS CLI

Para modificar una instancia específica de Amazon DocumentDB mediante la AWS CLI, utilice la `modify-db-instance` con los siguientes parámetros. Para obtener más información, consulte ModifyDBInstance. El siguiente código modifica la clase de instancia a `db.r5.large` para la instancia `sample-instance`.

Parámetros

- **`--db-instance-identifier`**: obligatorio. El identificador de la instancia que se va a modificar.
- **`--db-instance-class`**: opcional. La nueva capacidad de memoria e informática de la instancia (por ejemplo, `db.r5.large`). No todas las clases de instancia están disponibles en todas las Regiones de AWS. Si modifica la clase de la instancia se produce una interrupción durante el cambio. El cambio se aplica durante la siguiente ventana de mantenimiento, a menos que `ApplyImmediately` se especifique como verdadera para esta solicitud.
- **`--apply-immediately`** o **`--no-apply-immediately`**: opcional. Especifica si esta modificación debe aplicarse inmediatamente o esperar hasta el próximo periodo de mantenimiento. Si se omite este parámetro, la modificación se realiza durante el siguiente período de mantenimiento.

Example

Para Linux, macOS o Unix:

```
aws docdb modify-db-instance \
       --db-instance-identifier sample-instance \
       --db-instance-class db.r5.large \
```

```
       --apply-immediately
```

Para Windows:

```
aws docdb modify-db-instance ^
       --db-instance-identifier sample-instance ^
       --db-instance-class db.r5.large ^
       --apply-immediately
```

La salida de esta operación será similar a lo que se indica a continuación.

```
{
    "DBInstances": [
        {
            "DBInstanceIdentifier": "sample-instance-1",
            "DBInstanceClass": "db.r5.large",
            "Engine": "docdb",
            "DBInstanceStatus": "modifying",
            "Endpoint": {
                "Address": "sample-instance-1.node.us-east-1.docdb.amazonaws.com",
                "Port": 27017,
                "HostedZoneId": "ABCDEFGHIJKLM"
            },
            "InstanceCreateTime": "2020-01-10T22:18:55.921Z",
            "PreferredBackupWindow": "02:00-02:30",
            "BackupRetentionPeriod": 1,
            "VpcSecurityGroups": [
                {
                    "VpcSecurityGroupId": "sg-abcd0123",
                    "Status": "active"
                }
            ],
            "AvailabilityZone": "us-east-1a",
            "DBSubnetGroup": {
                "DBSubnetGroupName": "default",
                "DBSubnetGroupDescription": "default",
                "VpcId": "vpc-abcd0123",
                "SubnetGroupStatus": "Complete",
                "Subnets": [
                    {
                        "SubnetIdentifier": "subnet-abcd0123",
                        "SubnetAvailabilityZone": {
                            "Name": "us-east-1a"
```

```
                        },
                        "SubnetStatus": "Active"
                    },
                    {
                        "SubnetIdentifier": "subnet-abcd0123",
                        "SubnetAvailabilityZone": {
                            "Name": "us-east-1b"
                        },
                        "SubnetStatus": "Active"
                    }
                ]
            },
            "PreferredMaintenanceWindow": "sun:10:57-sun:11:27",
            "PendingModifiedValues": {
                "DBInstanceClass": "db.r5.large"
            },
            "EngineVersion": "3.6.0",
            "AutoMinorVersionUpgrade": true,
            "PubliclyAccessible": false,
            "DBClusterIdentifier": "sample-cluster",
            "StorageEncrypted": true,
            "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/wJalrXUtnFEMI/
K7MDENG/bPxRfiCYEXAMPLEKEY",
            "DbiResourceId": "db-ABCDEFGHIJKLMNOPQRSTUVWXYZ",
            "CACertificateIdentifier": "rds-ca-2019",
            "PromotionTier": 1,
            "DBInstanceArn": "arn:aws:rds:us-east-1:123456789012:db:sample-
instance-1",
            "EnabledCloudwatchLogsExports": [
                "profiler"
            ]
        }
    ]
}
```

Las modificaciones pueden tardar unos minutos en aplicarse. Solo puede usar la instancia cuando su estado sea available (disponible). Puede monitorizar el estado de la instancia mediante la Consola de administración de AWS o la AWS CLI. Para obtener más información, consulte Supervisión del estado de un clúster de Amazon DocumentDB.

Reinicio de la instancia de Amazon DocumentDB

Es posible que en algún momento necesite reiniciar su instancia de Amazon DocumentDB, normalmente por razones de mantenimiento. Si realiza determinados cambios, como cambiar el grupo de parámetros de clúster asociado a un clúster, debe reiniciar las instancias del clúster para que los cambios surtan efecto. Puede reiniciar una instancia especificada mediante la Consola de administración de AWS o la AWS CLI.

Cuando se reinicia una instancia, se reinicia el servicio del motor de base de datos. Al reiniciar una instancia, se produce una interrupción momentánea, durante la cual su estado se establece en `rebooting`. Cuando finaliza el reinicio, se crea un evento de Amazon DocumentDB.

El reinicio de una instancia no produce una conmutación por error. Para conmutar por error un clúster de Amazon DocumentDB, utilice la Consola de administración de AWS o la operación `failover-db-cluster` de la AWS CLI. Para obtener más información, consulte Conmutación por error a Amazon DocumentDB.

No puede reiniciar su instancia si no tiene el estado disponible. La base de datos puede no estar disponible por varias razones, como una modificación solicitada anteriormente o una acción durante un periodo de mantenimiento. Para obtener más información acerca de los estados de las instancias, consulte Supervisión del estado de un clúster de Amazon DocumentDB.

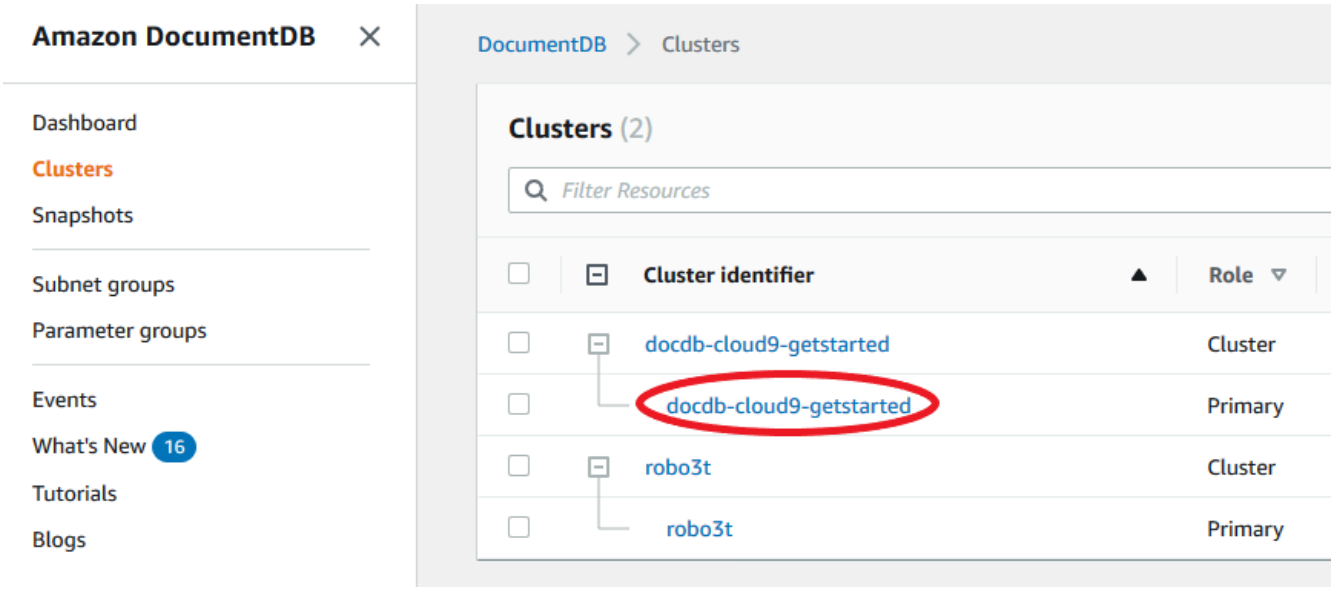
Using the Consola de administración de AWS

El siguiente procedimiento reinicia una instancia especificada mediante la consola.

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon DocumentDB en https://console.aws.amazon.com/docdb.
2. En el panel de navegación, seleccione Clusters (Clústeres).

   > **Tip**
   >
   > Si no ve el panel de navegación del lado izquierdo de la pantalla, seleccione el icono de menú
   > (≡)
   > en la esquina superior izquierda de la página.

3. En el cuadro de navegación de clústeres, verá la columna Identificador del clúster. Las instancias se muestran en clústeres, de forma similar a la siguiente captura de pantalla.



4. Marque la casilla de verificación situada a la izquierda de la instancia que desea reiniciar.
5. Elija Actions (Acciones), después Reboot (Reiniciar) y, por último, Reboot (Reiniciar) para confirmar el reinicio.

El reinicio de la instancia puede tardar unos minutos. Solo puede usar la instancia cuando su estado sea available (disponible). Puede monitorizar el estado de la instancia mediante la consola o la AWS CLI. Para obtener más información, consulte Supervisión del estado de un clúster de Amazon DocumentDB.

Using the AWS CLI

Para reiniciar una instancia de Amazon DocumentDB, utilice la operación `reboot-db-instance` con el parámetro `--db-instance-identifier`. Este parámetro especifica el identificador de la instancia que se va a reiniciar.

El siguiente código reinicia la instancia `sample-instance`.

Example

Para Linux, macOS o Unix:

```
aws docdb reboot-db-instance \
       --db-instance-identifier sample-instance
```

Para Windows:

```
aws docdb reboot-db-instance ^
       --db-instance-identifier sample-instance
```

La salida de esta operación será similar a lo que se indica a continuación.

```
{
    "DBInstance": {
        "DBInstanceIdentifier": "sample-instance",
        "DBInstanceClass": "db.r5.large",
        "Engine": "docdb",
        "DBInstanceStatus": "rebooting",
        "Endpoint": {
            "Address": "sample-instance.node.us-east-1.docdb.amazonaws.com",
            "Port": 27017,
            "HostedZoneId": "ABCDEFGHIJKLM"
        },
        "InstanceCreateTime": "2020-03-27T08:05:56.314Z",
        "PreferredBackupWindow": "02:00-02:30",
        "BackupRetentionPeriod": 1,
        "VpcSecurityGroups": [
            {
                "VpcSecurityGroupId": "sg-abcd0123",
                "Status": "active"
            }
        ],
        "AvailabilityZone": "us-east-1c",
        "DBSubnetGroup": {
            "DBSubnetGroupName": "default",
            "DBSubnetGroupDescription": "default",
            "VpcId": "vpc-abcd0123",
            "SubnetGroupStatus": "Complete",
            "Subnets": [
                {
                    "SubnetIdentifier": "subnet-abcd0123",
                    "SubnetAvailabilityZone": {
                        "Name": "us-east-1a"
                    },
                    "SubnetStatus": "Active"
                },
                {
                    "SubnetIdentifier": "subnet-wxyz0123",
                    "SubnetAvailabilityZone": {
                        "Name": "us-east-1b"
```

```
                    },
                    "SubnetStatus": "Active"
                }
            ]
        },
        "PreferredMaintenanceWindow": "sun:06:53-sun:07:23",
        "PendingModifiedValues": {},
        "EngineVersion": "3.6.0",
        "AutoMinorVersionUpgrade": true,
        "PubliclyAccessible": false,
        "DBClusterIdentifier": "sample-cluster",
        "StorageEncrypted": true,
        "KmsKeyId": "arn:aws:kms:us-east-1:<accountID>:key/sample-key",
        "DbiResourceId": "db-ABCDEFGHIJKLMNOPQRSTUVWXYZ",
        "CACertificateIdentifier": "rds-ca-2019",
        "PromotionTier": 1,
        "DBInstanceArn": "arn:aws:rds:us-east-1:<accountID>:db:sample-instance",
        "EnabledCloudwatchLogsExports": [
            "profiler"
        ]
    }
}
```

El reinicio de la instancia puede tardar unos minutos. Solo puede usar la instancia cuando su estado sea available (disponible). Puede monitorizar el estado de la instancia mediante la consola o la AWS CLI. Para obtener más información, consulte Supervisión del estado de un clúster de Amazon DocumentDB.

Eliminación de una instancia de Amazon DocumentDB

Puede eliminar su instancia de Amazon DocumentDB mediante la Consola de administración de AWS o la AWS CLI. Para eliminar una instancia, la instancia debe estar en el estado disponible. No puede eliminar una instancia detenida. Si el clúster de Amazon DocumentDB que contiene la instancia está detenido, inicie primero el clúster, espere a que la instancia esté disponible y, a continuación, elimine la instancia. Para obtener más información, consulte Detención e inicio de un clúster de bases de datos de Amazon DocumentDB.

> **Note**
>
> Amazon DocumentDB almacena todos los datos en el volumen del clúster. Los datos se conservan en ese volumen de clúster, incluso si elimina todas las instancias del clúster. Si necesita obtener acceso a los datos de nuevo, puede agregar una instancia al clúster en cualquier momento y reanudar el trabajo donde lo dejó.

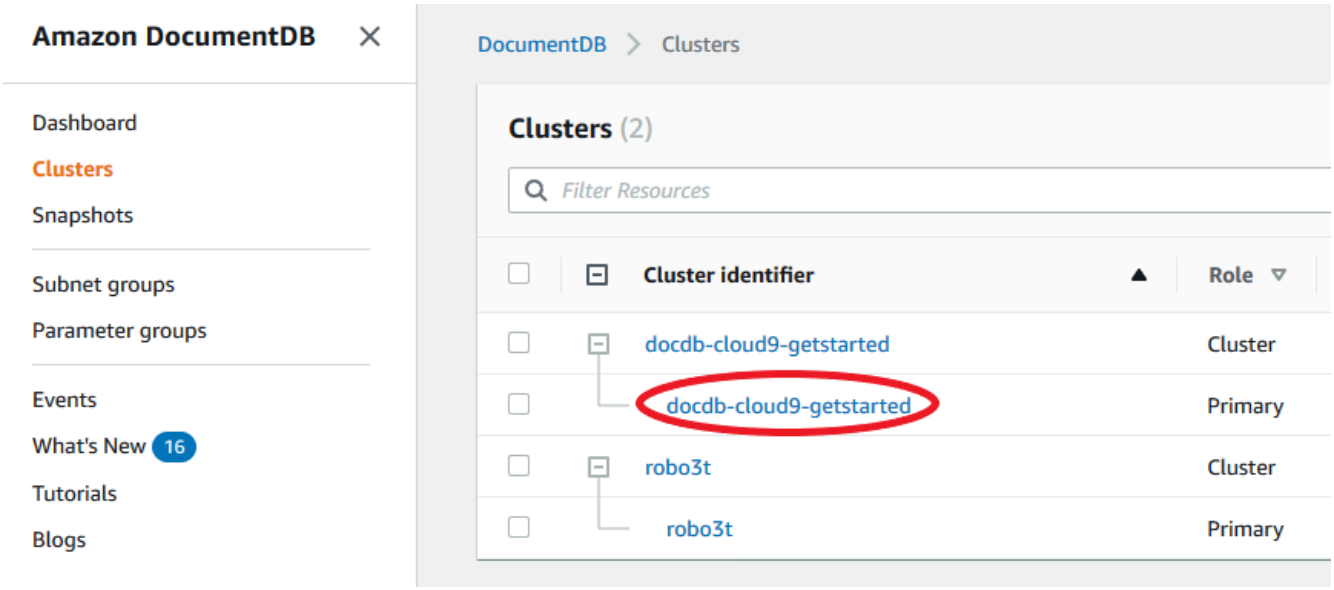
Using the Consola de administración de AWS

El siguiente procedimiento elimina una instancia de Amazon DocumentDB especificada mediante la consola.

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon DocumentDB en https://console.aws.amazon.com/docdb.
2. En el panel de navegación, seleccione Clusters (Clústeres).

   > **Tip**
   >
   > Si no ve el panel de navegación del lado izquierdo de la pantalla, seleccione el icono de menú
   > (≡)
   > en la esquina superior izquierda de la página.

3. En el cuadro de navegación de clústeres, verá la columna Identificador del clúster. Las instancias se muestran en clústeres, de forma similar a la siguiente captura de pantalla.



4. Marque la casilla de verificación situada a la izquierda de la instancia que desea eliminar.
5. Seleccione Acciones y, a continuación, elija Eliminar.

    1. Si va a eliminar la última instancia del clúster:
        - Create final cluster snapshot? (¿Crear instantánea de clúster final? Elija Sí si desea crear una instantánea final antes de eliminar el clúster. En caso contrario, elija No.
        - Nombre de la instantánea final: si ha decidido crear una instantánea final, escriba el identificador de la instantánea de clúster o de la nueva instantánea de clúster que se ha creado.
        - Delete <instance-name> instance? (¿Eliminar <nombre-de-la-instancia>? Escriba la frase Eliminar clúster completo en el campo para confirmar la eliminación.
    2. Si no va a eliminar la última instancia del clúster:
        - Delete <instance-name> instance? (¿Eliminar <nombre-de-la-instancia>? Escriba la frase Eliminarme en el campo para confirmar la eliminación.
6. Seleccione Delete (Eliminar) para eliminar la instancia.

La eliminación de una instancia tarda varios minutos. Para monitorear el estado de una instancia, consulte Supervisión del estado de un clúster de Amazon DocumentDB.

Using the AWS CLI

El siguiente procedimiento elimina una instancia de Amazon DocumentDB mediante la AWS CLI.

1. En primer lugar, determine cuántas instancias hay en el clúster de Amazon DocumentDB:

Para determinar cuántas instancias hay en el clúster, ejecute el comando `describe-db-clusters` de la siguiente manera.

```
aws docdb describe-db-clusters \
    --db-cluster-identifier sample-cluster \
    --query 'DBClusters[*].
[DBClusterIdentifier,DBClusterMembers[*].DBInstanceIdentifier]'
```

La salida de esta operación será similar a lo que se indica a continuación.

```
[
    [
        "sample-cluster",
        [
            "sample-instance-1",
            "sample-instance-2"
        ]
    ]
]
```

2. Si hay más de una instancia en el clúster de Amazon DocumentDB:

   Para eliminar una instancia de Amazon DocumentDB especificada, utilice el comando `delete-db-instance` con el parámetro `--db-instance-identifier`, como se muestra a continuación. La eliminación de una instancia tarda varios minutos. Para monitorear el estado de una instancia, consulte Supervisión del estado de un clúster de Amazon DocumentDB.

   ```
   aws docdb delete-db-instance \
          --db-instance-identifier sample-instance-2
   ```

   La salida de esta operación será similar a lo que se indica a continuación.

   ```
   {
       "DBInstance": {
           "DBInstanceIdentifier": "sample-instance-2",
           "DBInstanceClass": "db.r5.large",
           "Engine": "docdb",
           "DBInstanceStatus": "deleting",
           "Endpoint": {
               "Address": "sample-instance-2.node.us-east-1.docdb.amazonaws.com",
   ```

```
            "Port": 27017,
            "HostedZoneId": "ABCDEFGHIJKLM"
        },
        "InstanceCreateTime": "2020-03-27T08:05:56.314Z",
        "PreferredBackupWindow": "02:00-02:30",
        "BackupRetentionPeriod": 1,
        "VpcSecurityGroups": [
            {
                "VpcSecurityGroupId": "sg-abcd0123",
                "Status": "active"
            }
        ],
        "AvailabilityZone": "us-east-1c",
        "DBSubnetGroup": {
            "DBSubnetGroupName": "default",
            "DBSubnetGroupDescription": "default",
            "VpcId": "vpc-6242c31a",
            "SubnetGroupStatus": "Complete",
            "Subnets": [
                {
                    "SubnetIdentifier": "subnet-abcd0123",
                    "SubnetAvailabilityZone": {
                        "Name": "us-east-1a"
                    },
                    "SubnetStatus": "Active"
                },
                {
                    "SubnetIdentifier": "subnet-wxyz0123",
                    "SubnetAvailabilityZone": {
                        "Name": "us-east-1b"
                    },
                    "SubnetStatus": "Active"
                }
            ]
        },
        "PreferredMaintenanceWindow": "sun:06:53-sun:07:23",
        "PendingModifiedValues": {},
        "EngineVersion": "3.6.0",
        "AutoMinorVersionUpgrade": true,
        "PubliclyAccessible": false,
        "DBClusterIdentifier": "sample-cluster",
        "StorageEncrypted": true,
        "KmsKeyId": "arn:aws:kms:us-east-1:<accountID>:key/sample-key",
        "DbiResourceId": "db-ABCDEFGHIJKLMNOPQRSTUVWXYZ",
```

```
        "CACertificateIdentifier": "rds-ca-2019",
        "PromotionTier": 1,
        "DBInstanceArn": "arn:aws:rds:us-east-1:<accountID>:db:sample-instance-2",
        "EnabledCloudwatchLogsExports": [
            "profiler"
        ]
    }
}
```

3. Si la instancia que desea eliminar es la última instancia del clúster de Amazon DocumentDB:

   Si elimina la última instancia de un clúster de Amazon DocumentDB, también elimina ese clúster, así como las instantáneas automáticas y las copias de seguridad continuas asociadas a ese clúster.

   Para eliminar la última instancia del clúster, puede eliminar el clúster y, si lo desea, crear una instantánea final. Para obtener más información, consulte Eliminación de un clúster de Amazon DocumentDB.

Protección contra eliminación

Al eliminar la última instancia de un clúster de Amazon DocumentDB, también se eliminará el clúster, así como las instantáneas automáticas y las copias de seguridad continuas asociadas a ese clúster. Amazon DocumentDB aplica la protección contra eliminación para un clúster si realiza la operación de eliminación mediante la Consola de administración de AWS o la AWS CLI. Si la protección contra eliminación está habilitada, no podrá eliminar un clúster.

Para eliminar un clúster con la protección contra eliminación habilitada, primero debe modificar el clúster y deshabilitar la protección contra eliminación. Para obtener más información, consulte Eliminación de un clúster de Amazon DocumentDB.

Administración de clases de instancias

La clase de instancia de base de datos determina la capacidad de cómputo y de memoria de una instancia de Amazon DocumentDB (compatible con MongoDB). La clase de instancia que necesita depende de la potencia de procesamiento y de los requisitos de memoria.

Amazon DocumentDB admite las familias de clases de instancias R4, R5, R6G, R8G, T3 y T4G. Se trata de clases de instancias de la generación actual que se han optimizado para las aplicaciones

que hacen un uso intensivo de la memoria. Para conocer las especificaciones de estas clases, consulte Especificaciones de clases de instancias.

Temas

- Determinación de la clase de una instancia
- Cambio de la clase de una instancia
- Clases de instancias admitidas por región
- Especificaciones de clases de instancias

Determinación de la clase de una instancia

Para determinar la clase de una instancia, puedes usar la `describe-db-instances` AWS CLI operación Consola de administración de AWS o.

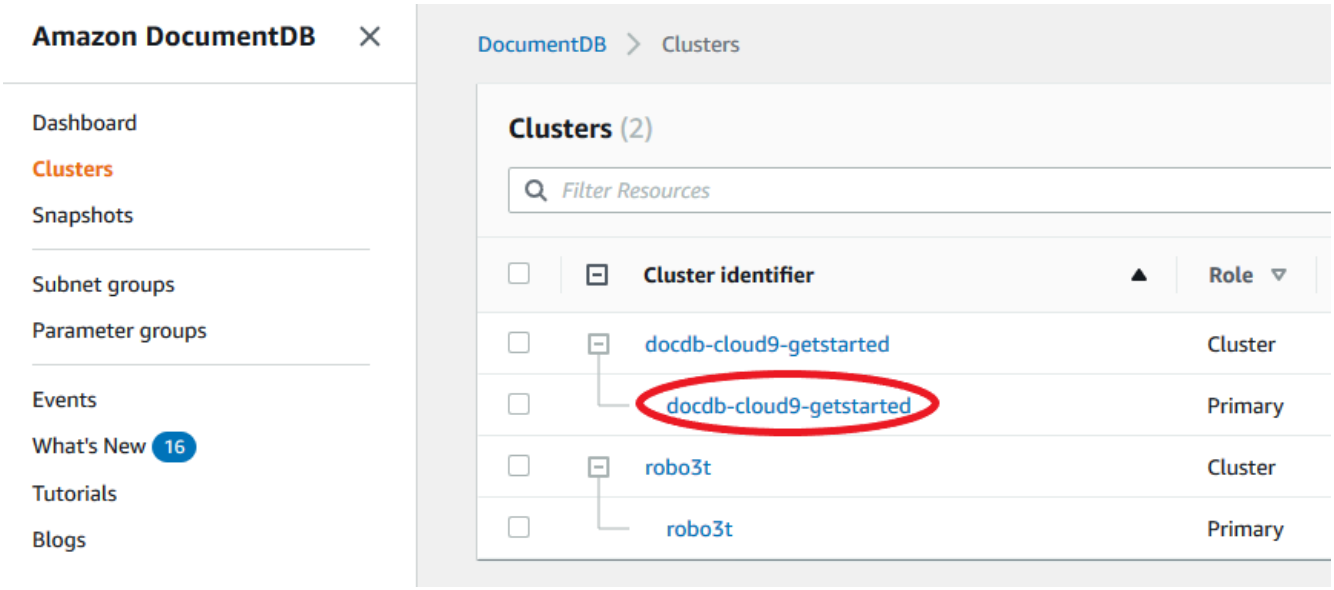
Using the Consola de administración de AWS

Para determinar la clase de instancia de las instancias del clúster, complete los siguientes pasos en la consola.

1. Inicie sesión en y abra la Consola de administración de AWS consola de Amazon DocumentDB en https://console.aws.amazon.com /docdb.
2. Para encontrar la instancia que le interesa, elija Clústeres en el panel de navegación.

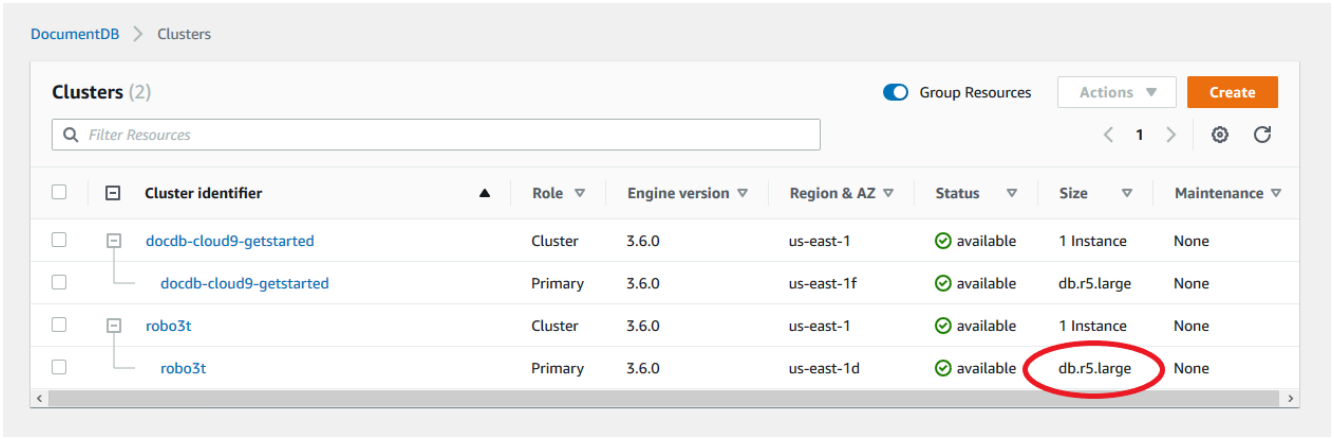
   > **Tip**
   >
   > Si no ve el panel de navegación del lado izquierdo de la pantalla, seleccione el icono de menú
   > (≡)
   > en la esquina superior izquierda de la página.

3. En el cuadro de navegación de clústeres, verá la columna Identificador del clúster. Las instancias se muestran en clústeres, de forma similar a la siguiente captura de pantalla.



4. En la lista de instancias, expande el clúster para encontrar las instancias que le interesan. Encuentre la instancia que desee. A continuación, fíjese en la columna Tamaño de la fila correspondiente a la instancia.

   En la imagen siguiente, la clase de la instancia `robo3t` es `db.r5.4xlarge`.



Using the AWS CLI

Para determinar la clase de una instancia mediante el AWS CLI, utilice la `describe-db-instances` operación con los siguientes parámetros.

- **`--db-instance-identifier`**— Opcional. Especifica la instancia para la que desea encontrar la clase de instancia. Si se omite este parámetro, `describe-db-instances` devuelve una descripción para un máximo de 100 instancias.

- **`--query`**: opcional. Especifica los miembros de la instancia que se van a incluir en los resultados. Si se omite este parámetro, se devuelven todos los miembros de la instancia.

Example

En el siguiente ejemplo se busca el nombre y la clase de la instancia para la instancia `sample-instance-1`.

Para Linux, macOS o Unix:

```
aws docdb describe-db-instances \
    --query 'DBInstances[*].[DBInstanceIdentifier,DBInstanceClass]' \
    --db-instance-identifier sample-instance-1
```

Para Windows:

```
aws docdb describe-db-instances ^
    --query 'DBInstances[*].[DBInstanceIdentifier,DBInstanceClass]' ^
    --db-instance-identifier sample-instance-1
```

La salida de esta operación será similar a lo que se indica a continuación.

```
[
    [
        "sample-instance-1",
        "db.r5.large"
    ]
```

Example

En el siguiente ejemplo se busca el nombre y la clase de la instancia para un máximo de 100 instancias de Amazon DocumentDB.

Para Linux, macOS o Unix:

```
aws docdb describe-db-instances \
    --query 'DBInstances[*].[DBInstanceIdentifier,DBInstanceClass]' \
    --filter Name=engine,Values=docdb
```

Para Windows:

```
aws docdb describe-db-instances ^
    --query 'DBInstances[*].[DBInstanceIdentifier,DBInstanceClass]' ^
    --filter Name=engine,Values=docdb
```

La salida de esta operación será similar a lo que se indica a continuación.

```
[
    [
        "sample-instance-1",
        "db.r5.large"
    ],
    [
        "sample-instance-2",
        "db.r5.large"
    ],
    [
        "sample-instance-3",
        "db.r5.4xlarge"
    ],
    [
        "sample-instance-4",
        "db.r5.4xlarge"
    ]
]
```

Para obtener más información, consulte Descripción de las instancias de Amazon DocumentDB.

Cambio de la clase de una instancia

Puede cambiar la clase de instancia de su instancia mediante el Consola de administración de AWS o el AWS CLI. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon DocumentDB.

Clases de instancias admitidas por región

Amazon DocumentDB admite las siguientes clases de instancia:

- R8G—Instancias optimizadas para memoria de última generación equipadas con procesadores AWS Graviton4 basados en ARM, que ofrecen un rendimiento hasta un 30% superior al de las instancias R6G.

- R6G—Instancias optimizadas para memoria equipadas con procesadores AWS Graviton2 basados en ARM que ofrecen un rendimiento hasta un 30% superior al de las instancias R5 a un coste un 5% menor.
- R6GD—Instancias R6G optimizadas para memoria con almacenamiento local no volátil en unidades de estado sólido (SSD) basadas en memoria exprés () para datos efímeros. NVMe
- R5: instancias optimizadas para memoria que ofrecen un rendimiento hasta un 100 % superior al de las instancias R4 por el mismo coste de instancia.
- R4: instancias optimizadas para memoria de generación anterior.
- T4G—Un tipo de instancia de uso general, de última generación, con capacidad de ráfaga y bajo coste, equipada con procesadores AWS Graviton2 basados en ARM, que proporciona un nivel básico de rendimiento de la CPU, con una relación precio-rendimiento hasta un 35% superior a la de las instancias T3 y es ideal para ejecutar aplicaciones con un uso moderado de la CPU que sufren picos temporales de uso.
- T3: tipo de instancia de uso general y ampliables que proporcionan un nivel básico de rendimiento de la CPU con posibilidad de ampliar el uso de la CPU en cualquier momento durante el tiempo que sea necesario.

Para conocer las especificaciones detalladas de las clases de instancias, consulte Especificaciones de clases de instancias.

Una clase de instancia determinada se podría admitir o no en una región determinada. En la siguiente tabla, se especifica qué clases de instancias admite Amazon DocumentDB en cada región.

Clases de instancias admitidas por región

Region	R8G	R6GD	R6G	R5	R4	T4G	T3	Sin servidor
Este de EE. UU. (Ohio)	Soportado	Soportado	Soportado	Soportado	Soportado	Soportado	Soportado	compatible
Este de EE. UU. (Norte de Virginia)	Soportado	Soportado	Soportado	Soportado	Soportado	Soportado	Soportado	compatible

Region	R8G	R6GD	R6G	R5	R4	T4G	T3	Sin servidor
Oeste de EE. UU. (Oregón)	Soportado	Soportado	Soportado	Soportado	Soportado	Soportado	Soportado	compatible
África (Ciudad del Cabo)			Soportado	Soportado		Soportado	Soportado	compatible
América del Sur (São Paulo)		Soportado	Soportado	Soportado		Soportado	Soportado	compatible
Asia-Pacífico (Hong Kong)			Soportado	Soportado		Soportado	Soportado	compatible
Asia-Pacífico (Hyderabad)			Soportado	Soportado		Soportado	Soportado	compatible
Asia-Pacífico (Malasia)			Soportado			Soportado	compatible	
Asia-Pacífico (Mumbai)	Soportado	Soportado	Soportado	Soportado		Soportado	Soportado	compatible
Asia-Pacífico (Osaka)		Soportado	Soportado	Soportado		Soportado	compatible	
Asia-Pacífico (Seúl)	Soportado	Soportado	Soportado	Soportado		Soportado	Soportado	compatible
Asia-Pacífico (Sídney)	Soportado	Soportado	Soportado	Soportado		Soportado	Soportado	compatible
Asia-Pacífico (Yakarta)	Soportado	Soportado	Soportado	Soportado		Soportado	compatible	
Asia-Pacífico (Singapur)	Soportado	Soportado	Soportado	Soportado		Soportado	Soportado	compatible

Region	R8G	R6GD	R6G	R5	R4	T4G	T3	Sin servidor
Asia-Pacífico (Tailandia)			Soportado			Soportado	compatible	
Asia-Pacífico (Tokio)	Soportado	Soportado	Soportado	Soportado		Soportado	Soportado	compatible
Canadá (centro)		Soportado	Soportado	Soportado		Soportado	Soportado	compatible
Europa (Fráncfort)	Soportado	Soportado	Soportado	Soportado		Soportado	Soportado	compatible
Europa (Irlanda)	Soportado	Soportado	Soportado	Soportado	Soportado	Soportado	Soportado	compatible
Europa (Londres)		Soportado	Soportado	Soportado		Soportado	Soportado	compatible
Europa (Milán)			Soportado	Soportado		Soportado	Soportado	compatible
Europa (París)		Soportado	Soportado	Soportado		Soportado	Soportado	compatible
Europa (España)	Soportado	Soportado	Soportado	Soportado		Soportado	Soportado	compatible
Europa (Estocolmo)	Soportado	Soportado	Soportado	Soportado		Soportado	compatible	
México (centro)			Soportado			Soportado	compatible	
Medio Oriente (EAU)			Soportado	Soportado		Soportado	Soportado	compatible

Region	R8G	R6GD	R6G	R5	R4	T4G	T3	Sin servidor
China (Pekín)		Soportado	Soportado	Soportado		Soportado	Soportado	compatible
China (Ningxia)			Soportado	Soportado		Soportado	Soportado	compatible
Israel (Tel Aviv)			Soportado	Soportado		Soportado	Soportado	compatible
AWS GovCloud (Oeste de EE. UU.)	Soportado	Soportado	Soportado	Soportado		Soportado	Soportado	compatible
AWS GovCloud (EEUU-Este)		Soportado	Soportado	Soportado		Soportado	Soportado	compatible

Especificaciones de clases de instancias

La siguiente tabla proporciona información detallada de las clases de instancias de Amazon DocumentDB, incluidos los tipos de instancias que se admiten en cada clase. Puede encontrar explicaciones sobre cada columna de la tabla debajo de la tabla.

Clase de instancia	CPU virtuales[1]	Memoria (GiB)[2]	NVMe Caché SSD por niveles (GiB) 3	Temperatura máxima de almacenamiento (GiB) 4	Ancho de banda de base/con ampliación (Gbps)[5]	Motores compatibles[6]
R8G: clase de instancia optimizada para memoria de la generación actual basada en Graviton4						
`db.r8g.large`	2	16	-	30	0,937/12,5	5.0.0
`db.r8g.xlarge`	4	32	-	60	1,875/12,5	5.0.0

Clase de instancia	CPU virtuales[1]	Memoria (GiB)[2]	NVMe Caché SSD por niveles (GiB) 3	Temperatura máxima de almacenamiento (GiB) 4	Ancho de banda de base/con ampliación (Gbps)[5]	Motores compatibles[6]
db.r8g.2xlarge	8	64	-	121	3,75/15,0	5.0.0
db.r8g.4xlarge	16	128	-	243	7,5/15,0	5.0.0
db.r8g.8xlarge	32	256	-	488	15	5.0.0
db.r8g.12xlarge	48	384	-	732	22	5.0.0
db.r8g.16xlarge	64	512	-	987	30	5.0.0
R6G: clase de instancia optimizada para memoria de la generación actual basada en Graviton2						
db.r6g.large	2	16	-	32	0,75/10	4.0.0 y 5.0.0
db.r6g.xlarge	4	32	-	63	1,25/10	4.0.0 y 5.0.0
db.r6g.2xlarge	8	64	-	126	2.5/10	4.0.0 y 5.0.0
db.r6g.4xlarge	16	128	-	252	5.0/10	4.0.0 y 5.0.0
db.r6g.8xlarge	32	256	-	504	12	4.0.0 y 5.0.0

Clase de instancia	CPU virtuales[1]	Memoria (GiB)[2]	NVMe Caché SSD por niveles (GiB) 3	Temperatura máxima de almacenamiento (GiB) 4	Ancho de banda de base/con ampliación (Gbps)[5]	Motores compatibles[6]
db.r6g.12xlarge	48	384	-	756	20	4.0.0 y 5.0.0
db.r6g.16xlarge	64	512	-	1008	25	4.0.0 y 5.0.0
R6GD: clase de instancia NVMe respaldada por la generación actual basada en Graviton2						
db.r6gd.xlarge	4	32	173	64	1.25/10	Solo 5.0.0
db.r6gd.2xlarge	8	64	346	128	2,5/ 10	Solo 5.0.0
db.r6gd.4xlarge	16	128	694	256	5,0/ 10	5.0.0 únicamente
db.r6gd.8xlarge	32	256	1388	512	12	Solo 5.0.0
db.r6gd.12xlarge	48	384	2082	768	20	Solo 5.0.0
db.r6gd.16xlarge	64	512	2776	1024	25	Solo 5.0.0
R5: clases de instancia optimizada para memoria de generación anterior						
db.r5.large	2	16	-	31	0.75/10	3.6.0, 4.0.0 y 5.0.0

Clase de instancia	CPU virtuales[1]	Memoria (GiB)[2]	NVMe Caché SSD por niveles (GiB) 3	Temperatura máxima de almacenamiento (GiB) 4	Ancho de banda de base/con ampliación (Gbps)[5]	Motores compatibles[6]
db.r5.xlarge	4	32	-	62	1,25/10	3.6.0, 4.0.0 y 5.0.0
db.r5.2xlarge	8	64	-	124	2.5/10	3.6.0, 4.0.0 y 5.0.0
db.r5.4xlarge	16	128	-	249	5.0/10	3.6.0, 4.0.0 y 5.0.0
db.r5.8xlarge	32	256	-	504	10	3.6.0, 4.0.0 y 5.0.0
db.r5.12xlarge	48	384	-	748	12	3.6.0, 4.0.0 y 5.0.0
db.r5.16xlarge	64	512	-	1008	20	3.6.0, 4.0.0 y 5.0.0
db.r5.24xlarge	96	768	-	1500	25	3.6.0, 4.0.0 y 5.0.0
R4: clases de instancia optimizada para memoria de generación anterior						
db.r4.large	2	15,25	-	30	0,75/10	Solo 3.6.0
db.r4.xlarge	4	30,5	-	60	1,25/10	Solo 3.6.0
db.r4.2xlarge	8	61	-	120	2.5/10	Solo 3.6.0

Clase de instancia	CPU virtuales[1]	Memoria (GiB)[2]	NVMe Caché SSD por niveles (GiB) 3	Temperatura máxima de almacenamiento (GiB) 4	Ancho de banda de base/con ampliación (Gbps)[5]	Motores compatibles[6]
`db.r4.4xlarge`	16	122	-	240	5.0 /10	Solo 3.6.0
`db.r4.8xlarge`	32	244	-	480	10	Solo 3.6.0
`db.r4.16xlarge`	64	488	-	960	25	Solo 3.6.0
T4G: clases de instancia de rendimiento ampliable de última generación basadas en Graviton2						
`db.t4g.medium`	2	4	-	8.13	0,256/ 5	4.0.0 y 5.0.0
T3: clases de instancia de rendimiento ampliable de generación anterior						
`db.t3.medium`	2	4	-	7.5	0,256/5	3.6.0, 4.0.0 y 5.0.0

Clase de instancia	CPU virtuales[1]	Memoria (GiB)[2]	NVMe Caché SSD por niveles (GiB) 3	Temperatura máxima de almacenamiento (GiB) 4	Ancho de banda de base/con ampliación (Gbps)[5]	Motores compatibles[6]

1. vCPU: el número de unidades centrales de procesamiento virtuales ()CPUs. Una CPU virtual es una unidad de capacidad que se puede usar para comparar clases de instancias. En lugar de comprar o arrendar un procesamiento concreto para usarlo durante varios meses o años, la capacidad se alquila por horas. Nuestro objetivo es proporcionar una cantidad constante de capacidad de CPU sea cual sea el hardware subyacente.
2. Memoria (GiB): RAM, en gigabytes, que se asigna a la instancia. A menudo, hay una relación coherente entre memoria y vCPU.
3. NVMe Caché en niveles de la SSD: el espacio del volumen de la SSD, medido en gigabytes, asignado como caché extendida para almacenar datos efímeros. Esta caché solo está disponible en instancias respaldadas por copias. NVMe
4. Temperatura máxima de almacenamiento (GiB): el espacio, medido en gigabytes, que se asigna a la instancia para el almacenamiento temporal no persistente de archivos. En el caso NVMe de las instancias respaldadas, este almacenamiento se aloja en un volumen SSD NVMe basado. En todas las demás instancias, se aloja en Amazon Elastic Block Store (EBS).
5. Ancho de banda de base/con ampliación (Gbps): el ancho de banda con ampliación representa el ancho de banda máximo en gigabits por segundo. Divídalo entre 8 para obtener el rendimiento esperado en gigabytes por segundo. Las instancias de tamaño 4xlarge o menos tienen un ancho de banda de base. Para satisfacer la demanda adicional, pueden utilizar un mecanismo de I/O crédito de red para superar su ancho de banda de referencia. Las instancias pueden utilizar la banda ancha de fragmentación durante un tiempo limitado, normalmente de 5 a 60 minutos, en función del tamaño de la instancia.
6. Motores compatibles: los motores de Amazon DocumentDB que admiten la clase de instancia.

Instancias respaldadas por NVMe

Las instancias respaldadas por NVMe ofrecen un rendimiento de consultas hasta 7 veces más rápido para aplicaciones con conjuntos de datos grandes que superan la memoria de una instancia normal. Estas instancias aprovechan el almacenamiento local en unidades de estado sólido (SSD) basado en

memoria rápida no volátil (NVMe) disponible en las instancias r6gd para almacenar datos efímeros, lo que reduce el acceso al almacenamiento en red y mejora la latencia de lectura y el rendimiento.

El espacio de la SSD local se divide en dos secciones:

- Caché por niveles: aproximadamente el 73 % de la SSD local se asigna como caché de base de datos, lo que permite al sistema almacenar hasta cinco veces más páginas de base de datos que la memoria principal por sí sola. La SSD local actúa como caché de segundo nivel, mientras que la caché del búfer en memoria existente sigue siendo la caché de primer nivel. La consulta accede solamente al almacenamiento externo si se produce un error tanto en la caché de búfer como en la de la SSD.
- Almacenamiento temporal: el 27 % restante se reserva para el almacenamiento temporal no persistente de archivos, que se utiliza para consultas complejas que implican ordenaciones u operaciones con consumo intensivo de recursos, como la compilación de índices. En instancias normales, el espacio temporal se encuentra en un volumen de Amazon Elastic Block Store (EBS). El almacenamiento temporal alojado localmente en la SSD reduce hasta dos veces la latencia de las consultas que implican ordenaciones y acelera las operaciones con consumo intensivo de recursos, como la compilación de índices.

Los detalles sobre el tipo de instancias respaldadas por NVMe compatibles y sus especificaciones se encuentran en Especificaciones de clases de instancias.

Temas

- Casos de uso recomendados para instancias respaldadas por NVMe
- Uso de instancias respaldadas por NVMe con Amazon DocumentDB
- Supervisión de instancias respaldadas por NVMe

Casos de uso recomendados para instancias respaldadas por NVMe

Le recomendamos utilizar instancias respaldadas por NVMe en las siguientes situaciones:

- Cargas de trabajo de lectura intensiva: si su carga de trabajo es de lectura intensiva y su conjunto de datos es más grande que la caché del búfer, lo que se refleja en métricas bajas de `BufferCacheHitRatio` y métricas altas de `ReadIOPS`, las instancias respaldadas por NVMe pueden ofrecer ventajas de rendimiento.
- Cargas de trabajo con actualización intensiva: si su carga de trabajo es de actualizaciones intensivas y la recopilación de elementos no utilizados no puede mantener el ritmo debido a la

latencia de lectura en el almacenamiento de red, las instancias respaldadas por NVMe podrían ayudar a mitigar el problema.

Las instancias respaldadas por NVMe pueden ser beneficiosas en varios casos de uso, entre los que se incluyen los siguientes:

- Aplicaciones a escala de Internet: las aplicaciones como el procesamiento de pagos, la facturación y el comercio electrónico con Acuerdos de nivel de servicio (SLA) de rendimiento estrictos pueden aprovechar las ventajas de rendimiento de las instancias respaldadas por NVMe.
- Paneles de informes en tiempo real: los paneles que ejecutan cientos de consultas para la recopilación de métricas/datos pueden beneficiarse de la baja latencia y el alto rendimiento de las instancias respaldadas por NVMe.
- Aplicaciones de IA generativa: las aplicaciones que utilizan la búsqueda vectorial para encontrar vecinos exactos o más cercanos entre millones de incrustaciones vectoriales pueden aprovechar el alto rendimiento de las instancias respaldadas por NVMe.

Uso de instancias respaldadas por NVMe con Amazon DocumentDB

Cómo usar instancias de Amazon DocumentDB respaldadas por NVMe:

- Cree un clúster de Amazon DocumentDB y añada una de las clases de instancia respaldadas por NVMe. Para obtener más información, consulte Creación de un clúster de Amazon DocumentDB.
- Como alternativa, modifique un clúster de Amazon DocumentDB existente para utilizar una de las clases de instancia respaldadas por NVMe. Para obtener más información, consulte Modificación de un clúster de Amazon DocumentDB.

Para comprobar la disponibilidad de las instancias respaldadas por NVMe en diferentes regiones de AWS, consulte Clases de instancias admitidas por región.

Si desea volver a cambiar de una instancia respaldada por NVMe a una instancia normal, modifique la clase de instancia de base de datos de su instancia de Amazon DocumentDB por una clase de instancia similar sin el almacenamiento de NVMe. Por ejemplo, si la clase de instancia actual es «db.r6gd.4xlarge», elija «db.r6g.4xlarge» para volver atrás. Para obtener más información, consulte Modificación de un clúster de Amazon DocumentDB.

Supervisión de instancias respaldadas por NVMe

Además de las métricas de instancia normales disponibles en Amazon CloudWatch, las instancias respaldadas por NVMe emiten métricas adicionales específicas para el almacenamiento en SSD basado en NVMe, las IOPS y el rendimiento.

```
NVMeStorageCacheHitRatio
FreeNVMeStorage
ReadIOPSNVMeStorage
ReadLatencyNVMeStorage
ReadThroughputNVMeStorage
WriteIOPSNVMeStorage
WriteLatencyNVMeStorage
WriteThroughputNVMeStorage
```

Para obtener más información acerca de estas métricas, consulte NVMe-métricas de instancias respaldadas

Administración de grupos de subredes de Amazon DocumentDB

Una nube privada virtual (VPC) es una red virtual dedicada para su Cuenta de AWS. Esta infraestructura en la nube está aislada lógicamente de otras redes virtuales de la nube de AWS. Puede lanzar sus recursos de AWS como por ejemplo clústeres de Amazon DocumentDB en su VPC de Amazon. Puede especificar un intervalo de direcciones IP para la VPC, añadir subredes, asociar grupos de seguridad y configurar tablas de ruteo.

Una subred es un rango de direcciones IP en su VPC de Amazon. Puede lanzar recursos de AWS en una subred especificada. Utilice una subred pública para los recursos que deben conectarse a Internet. Utilice una subred privada para los recursos que no dispondrán de conexión a Internet. Para obtener más información sobre subredes públicas y privadas, consulte Conceptos básicos de VPC y subredes en la Guía de usuario de la Nube privada virtual de Amazon.

Un grupo de subredes de base de datos es una colección de subredes que se crean en una VPC y que después se asignan a los clústeres. Un grupo de subredes le permite especificar una VPC determinada a la hora de crear clústeres. Si utiliza el grupo de subredes `default`, este abarca todas las subredes de la VPC.

Cada grupo de subredes de base de datos debe tener subredes como mínimo en dos zonas de disponibilidad de una región de determinada. Cuando crea un clúster de base de datos en una VPC,

debe elegir un grupo de subredes de base de datos. Amazon DocumentDB utiliza ese grupo de subredes de base de datos y su zona de disponibilidad preferida para seleccionar una subred y una dirección IP dentro de esa subred con el fin de asociarla al clúster. Si se produce un error en la instancia principal, Amazon DocumentDB puede promover una instancia de réplica correspondiente para que se convierta en la nueva instancia principal. A continuación, puede crear una nueva instancia de réplica utilizando una dirección IP de la subred en la que se encontraba la instancia principal anterior.

Cuando Amazon DocumentDB crea una instancia en una VPC, asigna una interfaz de red al clúster utilizando la dirección IP seleccionada del grupo de subredes de base de datos. Recomendamos que utilice el nombre de DNS, ya que la dirección IP subyacente puede cambiar durante la conmutación por error. Para obtener más información, consulte Puntos de conexión de Amazon DocumentDB.

Para obtener información sobre la creación de su propia VPC y sus subredes, consulte Uso de VPC y subredes en la Guía del usuario de la nube privada virtual de Amazon.

Temas

- Creación de un grupo de subredes de Amazon DocumentDB
- Descripción de un grupo de subredes de Amazon DocumentDB
- Modificación de un grupo de subredes de Amazon DocumentDB
- Eliminación de un grupo de subredes de Amazon DocumentDB

Creación de un grupo de subredes de Amazon DocumentDB

Al crear un clúster de Amazon DocumentDB, debe elegir una VPC de Amazon y el grupo de subredes correspondiente dentro de la VPC de Amazon para lanzar el clúster. Las subredes determinan la zona de disponibilidad y el rango de direcciones IP de la zona de disponibilidad que se deben utilizar para lanzar una instancia.

Un subgrupo de subredes es un determinado grupo de subredes (o AZ) que le permite especificar las zonas de disponibilidad que desea utilizar para lanzar instancias de Amazon DocumentDB. Por ejemplo, en un clúster con tres instancias, se recomienda que cada una de dichas instancias esté aprovisionada en una zona de disponibilidad (AZ) distinta, al hacerlo, optimiza la alta disponibilidad. De esa forma, si una de las AZ falla, solo se verá afectada una sola instancia.

Actualmente, las instancias de Amazon DocumentDB pueden aprovisionarse en hasta tres zonas de disponibilidad. Aunque un grupo de subredes tenga más de tres subredes, solo podrá utilizar tres

de esas subredes para crear un clúster de Amazon DocumentDB. Por ello, es recomendable que al crear un grupo de subredes solo elija las tres subredes en las que desee implementar las instancias.

Por ejemplo: se crea un clúster y Amazon DocumentDB elige las AZ {1A, 1B y 1C}. Si intenta crear una instancia en la AZ {1D}, la llamada a la API no funcionará correctamente. Sin embargo, si decide crear una instancia sin especificar la zona de disponibilidad concreta, Amazon DocumentDB elegirá una zona de disponibilidad por usted. Amazon DocumentDB utiliza un algoritmo para equilibrar la carga de las instancias en las AZ para ayudarle a obtener una alta disponibilidad. Si se aprovisionan tres instancias, de forma predeterminada se repartirán entre tres zonas de disponibilidad en lugar de aprovisionar todas ellas en una única AZ.

Prácticas recomendadas

- A menos que tenga un motivo específico, cree siempre un grupo de subredes con tres subredes. Lo anterior asegurará que los clústeres con tres o más instancias podrán lograr una mayor disponibilidad, debido a que las instancias se aprovisionarán en tres zonas de disponibilidad.
- Reparta siempre las instancias en varias zonas de disponibilidad para lograr una alta disponibilidad. Nunca ponga todas las instancias de un clúster en una única zona de disponibilidad.
- Debido a que pueden producirse eventos de conmutación por error en cualquier momento, no debe dar por hecho que una instancia principal o las instancias de réplica siempre estarán en una AZ determinada.

Cómo crear un grupo de subredes

Puede utilizar la Consola de administración de AWS o la AWS CLI para crear un grupo de subredes de Amazon DocumentDB:

Using the Consola de administración de AWS

Siga los siguientes pasos para crear un grupo de subredes de Amazon DocumentDB.

Creación de un grupo de subredes de Amazon DocumentDB

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon DocumentDB en https://console.aws.amazon.com/docdb.
2. En el panel de navegación, elija Subnet groups (Grupos de subredes)y, a continuación, elija Create (Crear).

> **Tip**
>
> Si no ve el panel de navegación del lado izquierdo de la pantalla, seleccione el icono de menú
> (≡)
> en la esquina superior izquierda de la página.

3. En la página Create subnet group (Crear grupo de subredes):

   a. En la sección Subnet group details (Detalles del grupo de subredes):

      i. Nombre: introduzca un nombre significativo para el grupo de la subred.

      ii. Description (Descripción): introduzca una descripción del grupo de subredes.

   b. En la sección Add subnets (Añadir subredes):

      i. VPC: elija una VPC de la lista, para este grupo de subredes.

      ii. Realice una de las siguientes acciones:

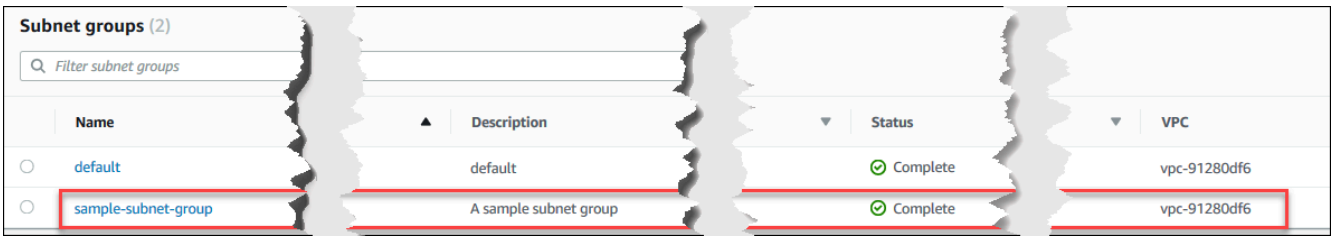
      - Para incluir todas las subredes en la VPC seleccionada, elija Add all the subnets related to this VPC (Añadir todas las subredes asociadas a esta VPC).
      - Para especificar subredes para este grupo de subredes, realice los pasos siguientes para cada zona de disponibilidad para la que desee incluir subredes. Debe incluir al menos dos zonas de disponibilidad.

        A. Zona de disponibilidad: de la lista, elija una zona de disponibilidad.

        B. Subred: de la lista, elija una subred de la zona de disponibilidad elegida para este grupo de subredes.

        C. Seleccione Add subnet (Añadir subred).

4. Seleccione Crear. Cuando se crea el grupo de subredes, se muestra junto con los demás grupos de subredes.



Using the AWS CLI

Para poder crear un grupo de subredes mediante la AWS CLI, primero debe determinar qué subredes se encuentran disponibles. Ejecute la siguiente operación de la AWS CLI para ver una lista de las zonas de disponibilidad y sus subredes.

Parámetros:

- **`--db-subnet-group`**: opcional. Si especifica un grupo de subredes concreto, puede ver las zonas de disponibilidad y las subredes de dicho grupo. Si omite este parámetro, puede ver las zonas de disponibilidad y las subredes de todos los grupos de subredes. Si especifica el grupo de subredes `default` puede ver todas las subredes de la VPC.

Example

Para Linux, macOS o Unix:

```
aws docdb describe-db-subnet-groups \
    --db-subnet-group-name default \
    --query 'DBSubnetGroups[*].[DBSubnetGroupName,Subnets[*].
[SubnetAvailabilityZone.Name,SubnetIdentifier]]'
```

Para Windows:

```
aws docdb describe-db-subnet-groups ^
    --db-subnet-group-name default ^
    --query 'DBSubnetGroups[*].[DBSubnetGroupName,Subnets[*].
[SubnetAvailabilityZone.Name,SubnetIdentifier]]'
```

La salida de esta operación será similar a lo que se indica a continuación (formato JSON).

```
[
    [
        "default",
        [
            [
                "us-east-1a",
                "subnet-4e26d263"
            ],
            [
                "us-east-1c",
```

```
                "subnet-afc329f4"
            ],
            [
                "us-east-1e",
                "subnet-b3806e8f"
            ],
            [
                "us-east-1d",
                "subnet-53ab3636"
            ],
            [
                "us-east-1b",
                "subnet-991cb8d0"
            ],
            [
                "us-east-1f",
                "subnet-29ab1025"
            ]
        ]
    ]
]
```

Si utiliza el resultado de la operación anterior, puede crear un nuevo grupo de subredes. El grupo de subredes nuevo debe incluir subredes de al menos dos zonas de disponibilidad.

Parámetros:

- **`--db-subnet-group-name`**: obligatorio. Nombre de este grupo de subredes.
- **`--db-subnet-group-description`**: obligatorio. Descripción de este grupo de subredes.
- **`--subnet-ids`**: obligatorio. Lista de las subredes que se van a incluir en este grupo de subredes. Ejemplo: : `subnet-53ab3636`.
- –Etiquetas: opcional. Lista de las etiquetas (pares clave-valor) que se van a asociar a este grupo de subredes.

El código siguiente crea el grupo de subredes `sample-subnet-group` con tres subredes, `subnet-4e26d263`, `subnet-afc329f4` y `subnet-b3806e8f`.

Para Linux, macOS o Unix:

```
aws docdb create-db-subnet-group \
    --db-subnet-group-name sample-subnet-group \
```

```
    --db-subnet-group-description "A sample subnet group" \
    --subnet-ids subnet-4e26d263 subnet-afc329f4 subnet-b3806e8f \
    --tags Key=tag1,Value=One Key=tag2,Value=2
```

Para Windows:

```
aws docdb create-db-subnet-group ^
    --db-subnet-group-name sample-subnet-group ^
    --db-subnet-group-description "A sample subnet group" ^
    --subnet-ids subnet-4e26d263 subnet-afc329f4 subnet-b3806e8f ^
    --tags Key=tag1,Value=One Key=tag2,Value=2
```

La salida de esta operación será similar a lo que se indica a continuación (formato JSON).

```
{
    "DBSubnetGroup": {
        "DBSubnetGroupDescription": "A sample subnet group",
        "DBSubnetGroupName": "sample-subnet-group",
        "Subnets": [
            {
                "SubnetAvailabilityZone": {
                    "Name": "us-east-1a"
                },
                "SubnetIdentifier": "subnet-4e26d263",
                "SubnetStatus": "Active"
            },
            {
                "SubnetAvailabilityZone": {
                    "Name": "us-east-1c"
                },
                "SubnetIdentifier": "subnet-afc329f4",
                "SubnetStatus": "Active"
            },
            {
                "SubnetAvailabilityZone": {
                    "Name": "us-east-1e"
                },
                "SubnetIdentifier": "subnet-b3806e8f",
                "SubnetStatus": "Active"
            }
        ],
        "VpcId": "vpc-91280df6",
```

```
        "DBSubnetGroupArn": "arn:aws:rds:us-east-1:123SAMPLE012:subgrp:sample-
subnet-group",
        "SubnetGroupStatus": "Complete"
    }
}
```

Descripción de un grupo de subredes de Amazon DocumentDB

Puede utilizar la Consola de administración de AWS o la AWS CLI para obtener detalles de un grupo de subredes de Amazon DocumentDB.

Using the Consola de administración de AWS

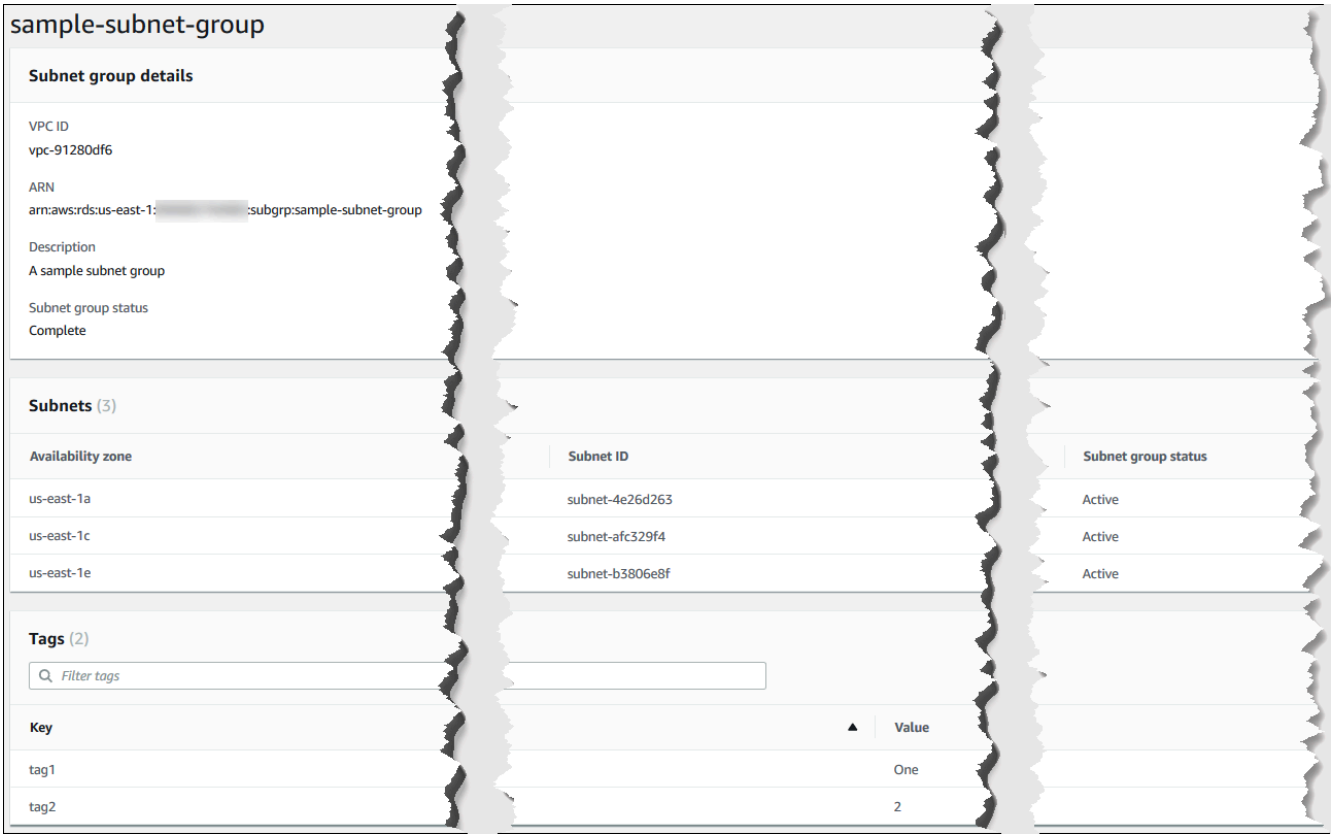
En el siguiente procedimiento se muestra cómo obtener detalles de un grupo de subredes de Amazon DocumentDB.

Para obtener los detalles de un grupo de subredes

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon DocumentDB en https://console.aws.amazon.com/docdb.
2. En el panel de navegación, elija Subnet groups (grupos de subredes).

   > **Tip**
   >
   > Si no ve el panel de navegación del lado izquierdo de la pantalla, seleccione el icono de menú
   > (≡)
   > en la esquina superior izquierda de la página.

3. Para consultar los detalles de un grupo de subredes seleccione el nombre de dicho grupo.



Using the AWS CLI

Para obtener los detalles de un grupo de subredes de Amazon DocumentDB, utilice la operación `describe-db-subnet-groups` con el siguiente parámetro.

Parámetro

- `--db-subnet=group-name`: opcional. Si se incluye, se muestran los detalles del grupo de subredes nombrado. Si se omite, se muestran los detalles de hasta 100 grupos de subredes.

Example

El siguiente código muestra los detalles del grupo de subredes `sample-subnet-group` que creamos en la sección Creación de un grupo de subredes de Amazon DocumentDB.

Para Linux, macOS o Unix:

```
aws docdb describe-db-subnet-groups \
    --db-subnet-group-name sample-subnet-group
```

Para Windows:

```
aws docdb describe-db-subnet-groups ^
    --db-subnet-group-name sample-subnet-group
```

La salida de esta operación será similar a lo que se indica a continuación (formato JSON).

```
{
    "DBSubnetGroup": {
        "DBSubnetGroupArn": "arn:aws:rds:us-east-1:123SAMPLE012:subgrp:sample-
subnet-group",
        "VpcId": "vpc-91280df6",
        "SubnetGroupStatus": "Complete",
        "DBSubnetGroupName": "sample-subnet-group",
        "Subnets": [
            {
                "SubnetAvailabilityZone": {
                    "Name": "us-east-1a"
                },
                "SubnetStatus": "Active",
                "SubnetIdentifier": "subnet-4e26d263"
            },
            {
                "SubnetAvailabilityZone": {
                    "Name": "us-east-1c"
                },
                "SubnetStatus": "Active",
                "SubnetIdentifier": "subnet-afc329f4"
            },
            {
                "SubnetAvailabilityZone": {
                    "Name": "us-east-1e"
                },
                "SubnetStatus": "Active",
                "SubnetIdentifier": "subnet-b3806e8f"
            }
        ],
        "DBSubnetGroupDescription": "A sample subnet group"
    }
}
```

Modificación de un grupo de subredes de Amazon DocumentDB

Puede utilizar la Consola de administración de AWS o la AWS CLI para modificar la descripción de un grupo de subredes o para añadir o eliminar subredes de un grupo de subredes de Amazon DocumentDB. Sin embargo, no puede modificar el grupo de subredes `default`.

Using the Consola de administración de AWS

Puede utilizar la Consola de administración de AWS para cambiar la descripción de un grupo de subredes o para añadir o eliminar subredes. Recuerde que, cuando termine, debe tener al menos dos zonas de disponibilidad asociadas al grupo de subredes.

Para modificar un grupo de subredes

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon DocumentDB en https://console.aws.amazon.com/docdb.
2. En el panel de navegación, elija Subnet groups (grupos de subredes). A continuación, elija el botón situado a la izquierda del nombre del grupo de subredes. Recuerde que no puede modificar el grupo de subredes `default`.

   > **Tip**
   >
   > Si no ve el panel de navegación del lado izquierdo de la pantalla, seleccione el icono de menú
   > (≡)
   > en la esquina superior izquierda de la página.

3. Elija Actions (Acciones) y después Modify (Modificar).
4. Descripción: para cambiar la descripción del grupo de subredes, introduzca una descripción nueva.
5. Para cambiar las subredes asociadas a un grupo de subredes, realice uno o varios de los siguientes pasos en la sección Add subnets (Añadir subredes):
   - Para eliminar todas las subredes de este grupo de subredes, seleccione Remove all (Eliminar todo).
   - Para eliminar subredes específicas de este grupo de subredes, seleccione Remove (Eliminar) en cada subred que desee eliminar.

- Para añadir todas las subredes asociadas a esta VPC, seleccione Add all the subnets related to this VPC (Añadir todas las subredes asociadas a esta VPC).
- Para añadir subredes específicas a este grupo de subredes, realice los siguientes pasos para cada zona de disponibilidad para la que desee añadir una subred.

  a. Zona de disponibilidad: de la lista, elija una nueva zona de disponibilidad.

  b. Subred: de la lista, elija una subred de la zona de disponibilidad elegida para este grupo de subredes.

  c. Seleccione Add subnet (Añadir subred).

6. En el cuadro de diálogo de confirmación:
   - Para hacer estos cambios en el grupo de subredes, elija Modify (Modificar).
   - Para que el grupo de subredes permanezca sin modificaciones, seleccione Cancel (Cancelar).

Using the AWS CLI

Puede utilizar la AWS CLI para cambiar la descripción de un grupo de subredes o para añadir o eliminar subredes. Recuerde que, cuando termine, debe tener al menos dos zonas de disponibilidad asociadas al grupo de subredes. No se puede modificar el grupo de subredes `default`.

Parámetros:

- `--db-subnet-group-name`: obligatorio. Nombre del grupo de subredes de Amazon DocumentDB que está modificando.
- `--subnet-ids`: obligatorio. Lista de las subredes que debe haber en el grupo de subredes después de realizar este cambio.

> **Important**
>
> Cualquier subred que actualmente se encuentre en el grupo de subredes y que no se incluya en esta lista se eliminará del grupo de subredes. Si desea mantener cualquiera de las subredes que actualmente se encuentra en el grupo de subredes, debe incluirla en esta lista.

- `--db-subnet-group-description`: opcional. Descripción del grupo de subredes.

Example

El siguiente código modifica la descripción y sustituye las subredes existentes por las subredes `subnet-991cb8d0`, `subnet-53ab3636` y `subnet-29ab1025`.

Para Linux, macOS o Unix:

```
aws docdb modify-db-subnet-group \
    --db-subnet-group-name sample-subnet-group \
    --subnet-ids subnet-991cb8d0 subnet-53ab3636 subnet-29ab1025 \
    --db-subnet-group-description "Modified subnet group"
```

Para Windows:

```
aws docdb modify-db-subnet-group ^
    --db-subnet-group-name sample-subnet-group ^
    --subnet-ids subnet-991cb8d0 subnet-53ab3636 subnet-29ab1025 ^
    --db-subnet-group-description "Modified subnet group"
```

La salida de esta operación será similar a lo que se indica a continuación (formato JSON). Tenga en cuenta que este es el mismo grupo de subredes que se creó en la sección Creación de un grupo de subredes de Amazon DocumentDB. Sin embargo, las subredes del grupo de subredes se sustituyen por las que se muestran en la operación `modify-db-subnet-group`.

```
{
    "DBSubnetGroup": {
        "DBSubnetGroupArn": "arn:aws:rds:us-east-1:123SAMPLE012:subgrp:sample-
subnet-group",
        "DBSubnetGroupDescription": "Modified subnet group",
        "SubnetGroupStatus": "Complete",
        "Subnets": [
            {
                "SubnetAvailabilityZone": {
                    "Name": "us-east-1d"
                },
                "SubnetStatus": "Active",
                "SubnetIdentifier": "subnet-53ab3636"
            },
            {
                "SubnetAvailabilityZone": {
                    "Name": "us-east-1b"
```

```
                },
                "SubnetStatus": "Active",
                "SubnetIdentifier": "subnet-991cb8d0"
            },
            {
                "SubnetAvailabilityZone": {
                    "Name": "us-east-1f"
                },
                "SubnetStatus": "Active",
                "SubnetIdentifier": "subnet-29ab1025"
            }
        ],
        "VpcId": "vpc-91280df6",
        "DBSubnetGroupName": "sample-subnet-group"
    }
}
```

Eliminación de un grupo de subredes de Amazon DocumentDB

Puede utilizar la Consola de administración de AWS o la AWS CLI para eliminar un grupo de subredes de Amazon DocumentDB. Sin embargo, no puede eliminar el grupo de subredes `default`.

Using the Consola de administración de AWS

Puede utilizar la Consola de administración de AWS para eliminar un grupo de subredes. Sin embargo, no se puede eliminar el grupo de subredes `default`.

Para eliminar un grupo de subredes

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon DocumentDB en https://console.aws.amazon.com/docdb.
2. En el panel de navegación, elija Subnet groups (grupos de subredes). A continuación, elija el botón situado a la izquierda del nombre del grupo de subredes. Recuerde que no puede eliminar el grupo de subredes `default`.

> **Tip**
>
> Si no ve el panel de navegación del lado izquierdo de la pantalla, seleccione el icono de menú

(≡)
en la esquina superior izquierda de la página.

3. Elija Acciones y, a continuación, elija Eliminar.
4. En el cuadro de diálogo de confirmación:
   - Para eliminar el grupo de subredes, seleccione Delete (Eliminar).
   - Para mantener el grupo de subredes, seleccione Cancel (Cancelar).

Using the AWS CLI

Para eliminar un grupo de subredes de Amazon DocumentDB mediante la AWS CLI, utilice la operación `delete-db-subnet-group` con el siguiente parámetro.

Parámetro

- `--db-subnet-group-name`: obligatorio. Nombre del grupo de subredes de Amazon DocumentDB que se va a eliminar. Recuerde que no puede eliminar el grupo de subredes `default`.

Example

El código siguiente elimina `sample-subnet-group`.

Para Linux, macOS o Unix:

```
aws docdb delete-db-subnet-group \
    --db-subnet-group-name sample-subnet-group
```

Para Windows:

```
aws docdb delete-db-subnet-group ^
    --db-subnet-group-name sample-subnet-group
```

Esta operación no produce ningún resultado.

Alta disponibilidad y replicación de Amazon DocumentDB

Puede conseguir un alto nivel de disponibilidad y escalado de lectura en Amazon DocumentDB (con compatibilidad con MongoDB) mediante instancias de réplica. Un único clúster de Amazon DocumentDB admite una sola instancia principal y hasta 15 instancias de réplica. Dichas instancias pueden distribuirse entre las zonas de disponibilidad dentro de la región del clúster. La instancia principal acepta el tráfico de lectura y escritura, y las instancias de réplica solo aceptan solicitudes de lectura.

El volumen del clúster consta de varias copias de los datos del clúster. Sin embargo, los datos del volumen del clúster se representan como un único volumen lógico para la instancia principal y para las réplicas de Amazon DocumentDB del clúster. Las instancias de réplica presentan consistencia final. Devuelven los resultados de las consultas con un retardo de réplica mínimo, normalmente muy inferior a 100 milisegundos una vez que la instancia principal ha escrito una actualización. El retardo de la réplica varía en función de la velocidad de cambio de la base de datos. Es decir, durante los periodos en los que se produce una gran cantidad de operaciones de escritura en la base de datos, puede registrarse un aumento del retardo de réplica.

Escalado de lectura

Las réplicas de Amazon DocumentDB funcionan bien para el escalado de lectura porque están totalmente dedicadas a las operaciones de lectura en el volumen del clúster. Las operaciones de escritura se administran en la instancia principal. El volumen del clúster lo comparten todas las instancias del clúster. Por lo tanto, no tiene que replicar y mantener una copia de los datos de cada réplica de Amazon DocumentDB.

Alta disponibilidad

Cuando se crea un clúster de Amazon DocumentDB, dependiendo del número de zonas de disponibilidad del grupo de subredes (debe haber al menos dos), Amazon DocumentDB aprovisiona instancias en las distintas zonas de disponibilidad. Cuando se crea las instancias del clúster, Amazon DocumentDB distribuye automáticamente las instancias entre las zonas de disponibilidad de un grupo de subredes para equilibrar el clúster. Esta acción también impide que todas las instancias se encuentren en la misma zona de disponibilidad.

Ejemplo

Para ilustrarlo, imagine un ejemplo en el que se crea un clúster que tiene un grupo de subredes con tres zonas de disponibilidad: AZ1, AZ y AZ3.

Cuando se crea la primera instancia del clúster, es la instancia principal y se sitúa en una de las zonas de disponibilidad. En este ejemplo, está en AZ1. La segunda instancia que se crea es una instancia de réplica y se sitúa en una de las otras dos zonas de disponibilidad, por ejemplo AZ2. La tercera instancia que se crea también es una instancia de réplica y se sitúa en la zona de disponibilidad restante, AZ3. Si se crean más instancias, estas se distribuyen entre las distintas zonas de disponibilidad para lograr el equilibrio en el clúster.

Si se produce un error en la instancia principal (AZ1), se activará una conmutación por error y una de las réplicas existentes pasará a ser la instancia principal. Cuando se recupere la antigua instancia principal, se convertirá en una réplica en la misma zona de disponibilidad en la que se aprovisionó (AZ1). Al suministrar un clúster de tres instancias, Amazon DocumentDB sigue conservando ese clúster de tres instancias. Amazon DocumentDB gestiona automáticamente la detección, la conmutación por error y la recuperación de los errores de las instancias sin ninguna intervención manual.

Cuando Amazon DocumentDB realiza una conmutación por error y recupera una instancia, la instancia recuperada permanece en la zona de disponibilidad en la que se aprovisionó originalmente. Sin embargo, el rol de la instancia podría cambiar de principal a réplica. Esto tiene por objeto evitar que una serie de conmutaciones por error pueda provocar que todas las instancias se encuentren en la misma zona de disponibilidad.

Puede especificar réplicas de Amazon DocumentDB para que actúen como destino para las conmutaciones por error. Es decir, si la instancia principal falla, la réplica de un tercero o la réplica de Amazon DocumentDB que ha especificado pasa a ser la instancia principal. En este proceso se produce una breve interrupción durante la cual las solicitudes de escritura y lectura realizadas a la instancia principal generan errores con una excepción. Si el clúster de Amazon DocumentDB no incluye ninguna réplica de Amazon DocumentDB; la instancia principal se vuelve cuando produce un error. Promover una réplica de Amazon DocumentDB es mucho más rápido que volver a crear la instancia principal.

Para escenarios de alta disponibilidad, le recomendamos que cree una o varias réplicas de Amazon DocumentDB. Dichas réplicas deberían ser de la misma clase de instancia que la instancia principal y estar en zonas de disponibilidad distintas para el clúster de Amazon DocumentDB.

Para obtener más información, consulte los siguientes temas:

- Información general de la tolerancia a errores de clúster de Amazon DocumentDB
- Conmutación por error a Amazon DocumentDB
  - Control del destino de la conmutación por error

Alta disponibilidad con clústeres globales

Para una alta disponibilidad en varias Regiones de AWS, puede configurar clústeres globales de Amazon DocumentDB. Cada clúster global abarca varias regiones, lo que permite lecturas globales de baja latencia y la recuperación de desastres de interrupciones en una Región de AWS. Amazon DocumentDB maneja automáticamente la reproducción de todos los datos y actualizaciones desde la región primaria a cada una de las regiones secundarias.

Adición de réplicas de

La primera instancia que se añade al clúster es la instancia principal. Cada instancia de base de datos que se añade después de la primera instancia es una instancia de réplica. Un clúster puede tener hasta 15 instancias de réplica, además de la instancia principal.

Cuando crea un clúster mediante la Consola de administración de AWS, se crea automáticamente una instancia principal al mismo tiempo. Para crear una réplica al mismo tiempo que crea el clúster y la instancia principal, seleccione Create replica in different zone (Crear réplica en zona diferente). Para obtener más información, consulte el paso 4.d de Creación de un clúster de Amazon DocumentDB. Para añadir más réplicas a un clúster de Amazon DocumentDB, consulte Agregación de una instancia de Amazon DocumentDB a un clúster.

Cuando usa la AWS CLI para crear el clúster, debe crear explícitamente la instancia principal y las instancias de réplica. Para obtener más información, consulte la sección "Mediante la AWS CLI" de los temas siguientes:

- Creación de un clúster de Amazon DocumentDB
- Agregación de una instancia de Amazon DocumentDB a un clúster

Conmutación por error a Amazon DocumentDB

En algunos casos, como en determinados tipos de mantenimiento planificado, o en el improbable caso de que se produzca un error en el nodo principal o en la zona de disponibilidad, Amazon DocumentDB (con compatibilidad con MongoDB) detectará el error y reemplazará el nodo principal. Durante una conmutación por error, el tiempo de inactividad de escritura se minimiza. Esto se debe a que el papel del nodo principal se conmuta por error a una de las réplicas de lectura en lugar de tener que crear y aprovisionar un nuevo nodo principal. Esta detección de error y promoción de réplica garantizan la posibilidad de reanudar la escritura en el nuevo principal tan pronto como se complete la promoción.

Para que la conmutación por error funcione, el clúster debe tener como mínimo dos instancias: una instancia principal y al menos una de réplica.

> **Note**
>
> Este tema solo se aplica a los clústeres basados en instancias de Amazon DocumentDB. No se aplica a los clústeres elásticos o globales.

Control del destino de la conmutación por error

Amazon DocumentDB proporciona niveles de conmutación por error como una forma de controlar qué instancia de réplica pasa a ser la instancia principal cuando se produce una conmutación por error.

Niveles de conmutación por error

Cada instancia de réplica está asociada a un nivel de conmutación por error (0-15). Cuando se produce una conmutación por error debido a tareas de mantenimiento o al caso improbable de que se produzca un error de hardware, la instancia principal se conmuta a una réplica con el nivel de prioridad mayor (el nivel más bajo). Si varias réplicas tienen el mismo nivel de prioridad, la instancia principal se conmutará a la réplica de ese nivel cuyo tamaño sea lo más similar a la principal anterior.

Estableciendo el nivel de conmutación por error para un grupo de réplicas seleccionadas en `0` (la prioridad más alta), puede asegurarse de que una conmutación por error promoverá una de las réplicas de ese grupo. En la práctica, puede evitar determinadas réplicas pasen a ser la instancia principal en caso de que se produzca una conmutación por error asignando un nivel de prioridad bajo (un número alto) a esas réplicas. Esto resulta útil en aquellos casos en los que determinadas réplicas se usan ampliamente en una aplicación y la conmutación por error a una de ellas afectaría negativamente a una aplicación crítica.

Puede configurar el nivel de conmutación por error de una instancia cuando la cree o modificándola más adelante. La configuración del nivel conmutación por error de una instancia modificando la instancia no genera una conmutación por error. Para obtener más información, consulte los siguientes temas:

- Agregación de una instancia de Amazon DocumentDB a un clúster
- Modificación de una instancia de base de datos de Amazon DocumentDB

Al iniciar manualmente una conmutación por error, dispone de dos métodos para controlar qué instancia de réplica pasa a ser la principal: los niveles de conmutación por error indicados anteriormente y el parámetro `--target-db-instance-identifier`.

--target-db-instance-identifier

Para las pruebas, puede forzar una conmutación por error mediante la operación `failover-db-cluster`. Puede utilizar el parámetro `--target-db-instance-identifier` para especificar qué réplica pasará a ser la instancia principal. El uso del parámetro `--target-db-instance-identifier` invalida el nivel de prioridad de conmutación por error. Si no especifica el parámetro `--target-db-instance-identifier`, la conmutación por error de la instancia principal se rige por el nivel de prioridad de conmutación por error.

¿Qué ocurre durante una conmutación por error?

Amazon DocumentDB administra automáticamente la conmutación por error para que sus aplicaciones puedan reanudar las operaciones de la base de datos lo antes posible y sin intervención administrativa.

- Si dispone de una réplica de Amazon DocumentDB en la misma zona de disponibilidad o en otra distinta cuando se realiza la conmutación por error, Amazon DocumentDB cambia el registro de nombre canónico (CNAME) para que su instancia apunte a la réplica en buen estado que, a su vez, se convierte en la nueva instancia principal. La conmutación por error suele completarse en 30 segundos de principio a fin.
- Si no tiene una instancia de réplica de Amazon DocumentDB (por ejemplo, un clúster de instancia única), Amazon DocumentDB intentará crear una nueva instancia en la misma zona de disponibilidad que la instancia original. Este reemplazo de la instancia original se lleva a cabo con el mayor esfuerzo, pero puede fallar si, por ejemplo, existe un problema que esté afectando a la zona de disponibilidad de manera generalizada.

La aplicación debe reintentar establecer las conexiones de la base de datos en caso de que se pierda la conexión.

Prueba de conmutación por error

Una conmutación por error de un clúster promueve una de las réplicas de Amazon DocumentDB (instancias de solo lectura) del clúster a instancia principal (la instancia de escritura del clúster).

Cuando se produce un error en la instancia principal, Amazon DocumentDB conmuta automáticamente a una réplica de Amazon DocumentDB, si existe. Puede forzar una conmutación por error cuando desee simular un error en una instancia principal para realizar pruebas. Cada instancia de un clúster tiene su propia dirección de punto de conexión. Por lo tanto, es necesario eliminar y restablecer las conexiones existentes que utilizan dichas direcciones de punto de conexión cuando finalice la conmutación por error.

Para forzar una conmutación por error, utilice la operación `failover-db-cluster` con los parámetros que se indican a continuación.

- `--db-cluster-identifier`: obligatorio. El nombre del clúster de base de datos que se va a conmutar por error.
- `--target-db-instance-identifier`: opcional. El nombre de la instancia que pasará a ser la instancia principal.

Example

La siguiente operación fuerza una conmutación por error del clúster `sample-cluster`. No especifica qué instancia se convertirá en la nueva instancia principal, por lo que Amazon DocumentDB elige la instancia de acuerdo con el nivel de prioridad de conmutación por error.

Para Linux, macOS o Unix:

```
aws docdb failover-db-cluster \
   --db-cluster-identifier sample-cluster
```

Para Windows:

```
aws docdb failover-db-cluster ^
   --db-cluster-identifier sample-cluster
```

La siguiente operación fuerza una conmutación por error del clúster `sample-cluster`, especificando que `sample-cluster-instance` pasará a ser la instancia principal. (Observe `"IsClusterWriter": true` en el resultado).

Para Linux, macOS o Unix:

```
aws docdb failover-db-cluster \
```

```
   --db-cluster-identifier sample-cluster \
   --target-db-instance-identifier sample-cluster-instance
```

Para Windows:

```
aws docdb failover-db-cluster ^
   --db-cluster-identifier sample-cluster ^
   --target-db-instance-identifier sample-cluster-instance
```

La salida de esta operación será similar a lo que se indica a continuación (formato JSON).

```
{
    "DBCluster": {
        "HostedZoneId": "Z2SUY0A1719RZT",
        "Port": 27017,
        "EngineVersion": "3.6.0",
        "PreferredMaintenanceWindow": "thu:04:05-thu:04:35",
        "BackupRetentionPeriod": 1,
        "ClusterCreateTime": "2018-06-28T18:53:29.455Z",
        "AssociatedRoles": [],
        "DBSubnetGroup": "default",
        "MasterUsername": "master-user",
        "Engine": "docdb",
        "ReadReplicaIdentifiers": [],
        "EarliestRestorableTime": "2018-08-21T00:04:10.546Z",
        "DBClusterIdentifier": "sample-cluster",
        "ReaderEndpoint": "sample-cluster.node.us-east-1.docdb.amazonaws.com",
        "DBClusterMembers": [
            {
                "DBInstanceIdentifier": "sample-cluster-instance",
                "DBClusterParameterGroupStatus": "in-sync",
                "PromotionTier": 1,
                "IsClusterWriter": true
            },
            {
                "DBInstanceIdentifier": "sample-cluster-instance-00",
                "DBClusterParameterGroupStatus": "in-sync",
                "PromotionTier": 1,
                "IsClusterWriter": false
            },
            {
                "DBInstanceIdentifier": "sample-cluster-instance-01",
                "DBClusterParameterGroupStatus": "in-sync",
```

```
                "PromotionTier": 1,
                "IsClusterWriter": false
            }
        ],
        "AvailabilityZones": [
            "us-east-1b",
            "us-east-1c",
            "us-east-1a"
        ],
        "DBClusterParameterGroup": "default.docdb3.6",
        "Endpoint": "sample-cluster.node.us-east-1.docdb.amazonaws.com",
        "IAMDatabaseAuthenticationEnabled": false,
        "AllocatedStorage": 1,
        "LatestRestorableTime": "2018-08-22T21:57:33.904Z",
        "PreferredBackupWindow": "00:00-00:30",
        "StorageEncrypted": false,
        "MultiAZ": true,
        "Status": "available",
        "DBClusterArn": "arn:aws:rds:us-east-1:123456789012:cluster:sample-cluster",
        "VpcSecurityGroups": [
            {
                "Status": "active",
                "VpcSecurityGroupId": "sg-12345678"
            }
        ],
        "DbClusterResourceId": "cluster-ABCDEFGHIJKLMNOPQRSTUVWXYZ"
    }
}
```

Retraso de replicación

El retraso de replicación suele ser de 50 ms o menos. Los motivos más comunes del aumento del retraso en la réplica son:

- Una velocidad de escritura alta en la principal que hace que las réplicas de lectura queden por detrás de la principal.
- Discrepancia en las réplicas de lectura entre consultas de larga duración (p. ej., escaneos secuenciales de gran tamaño o consultas de agregación) y la replicación de escritura entrante.
- Gran cantidad de consultas simultáneas en las réplicas de lectura.

Para minimizar el retraso en la replicación, pruebe estas técnicas de solución de problemas:

- Si tiene una alta velocidad de escritura o un uso elevado de la CPU, le recomendamos que escale verticalmente las instancias del clúster.
- Si hay consultas de larga duración en las réplicas de lectura y se actualizan con mucha frecuencia los documentos consultados, plantéese la posibilidad de modificar las consultas de larga duración o ejecutarlas en la réplica principal o de escritura para evitar problemas en las réplicas de lectura.
- Si hay un gran número de consultas simultáneas o un uso elevado de la CPU solo en las réplicas de lectura, otra opción es escalar horizontalmente el número de réplicas de lectura para distribuir la carga de trabajo.
- Dado que el retraso en la replicación se debe a un alto rendimiento de escritura y a que las consultas se ejecutan durante mucho tiempo, recomendamos solucionar el retraso de la replicación utilizando la métrica DBClusterReplicaLagMaximum CW en combinación con el registrador de consultas lentas y las métricas `WriteThroughput`/`WriteIOPS`.

En general, se recomienda que todas las réplicas sean del mismo tipo de instancia, de modo que una conmutación por error de un clúster no provoque una degradación del rendimiento.

Si va a elegir entre escalar verticalmente y horizontalmente (por ejemplo, seis instancias más pequeñas frente a tres instancias más grandes), normalmente recomendamos que primero intente escalar verticalmente (instancias más grandes) antes de hacerlo horizontalmente, ya que obtendrá una caché de búfer más grande por instancia de base de datos.

De forma proactiva, debe configurar una alarma de retraso de replicación y establecer su umbral en un valor que considere que es el límite superior del retraso (u “obsoleto”) que pueden estar los datos de las instancias de réplica antes de que comiencen a afectar a la funcionalidad de la aplicación. En general, le recomendamos que se supere el umbral de retraso de replicación en varios puntos de datos antes de emitir una alarma debido a las cargas de trabajo transitorias.

> **Note**
>
> Además, recomendamos que configure otra alarma para los retrasos de replicación que superen los 10 segundos. Si supera este umbral para varios puntos de datos, recomendamos que escale verticalmente las instancias o reduzca el rendimiento de la escritura en la instancia principal.

Administración de índices de Amazon DocumentDB

Temas

- Creación de índices de Amazon DocumentDB
- Mantenimiento de índices de Amazon DocumentDB

Creación de índices de Amazon DocumentDB

La compilación de índices en Amazon DocumentDB requiere tomar una serie de decisiones:

- ¿Con qué rapidez debe completarse?
- ¿Es posible que no se pueda acceder a la colección mientras se realiza la compilación?
- ¿Cuánta potencia de computación de una instancia se puede asignar a la compilación?
- ¿Qué tipo de índice se debe crear?

Esta sección le ayuda a responder a estas preguntas y proporciona los comandos y ejemplos de supervisión para crear un índice de Amazon DocumentDB en su colección de clústeres basada en instancias.

Directrices

Las siguientes pautas incluyen los límites básicos y las desventajas de configuración a la hora de crear nuevos índices:

- Compatibilidad con la versión de Amazon DocumentDB: si bien la indexación de un solo proceso de trabajo se admite en todas las versiones de Amazon DocumentDB, la indexación de varios procesos de trabajo solo se admite en las versiones 4.0 y 5.0 de Amazon DocumentDB.
- Compensación de rendimiento: aumentar el número de procesos de trabajo en el proceso de creación del índice aumenta la utilización de la CPU y la E/S de lectura en la instancia principal de la base de datos Amazon DocumentDB. Los recursos necesarios para crear un índice nuevo no estarán disponibles para su carga de trabajo en ejecución.
- Clústeres elásticos: la indexación em paralelo no se admite en los clústeres elásticos de Amazon DocumentDB.
- Número máximo de procesos de trabajo: el número máximo de procesos de trabajo que puede configurar depende del tamaño de la instancia principal en el clúster de base de datos. Es la mitad

del número total de v CPUs en la instancia principal del clúster de base de datos. Por ejemplo, puede ejecutar un máximo de 32 trabajadores en una instancia db.r6g.16xlarge que tenga 64 v. CPUs

> **Note**
>
> Los equipos de trabajo en paralelo no son compatibles con las clases de instancias 2xlarge y versiones anteriores.

- Número mínimo de procesos de trabajo: el número mínimo de procesos de trabajo que puede configurar es uno. La configuración predeterminada para la creación de índices en clústeres basados en instancias es de dos procesos de trabajo. Sin embargo, puede reducir el número de procesos de trabajo a uno mediante la opción “subprocesos de trabajo”. Esto ejecutará el proceso con un solo proceso de trabajo.
- Compresión de índices: Amazon DocumentDB no admite la compresión de índices. Los tamaños de datos para índices pueden ser superiores que cuando utiliza otras opciones.
- Indexación de varias colecciones: la mitad de la v CPUs de la instancia principal del clúster de base de datos se puede usar para los trabajadores configurados que crean índices en varias colecciones.
- Tipos de índices: consulte esta entrada de blog para obtener una explicación completa de los tipos de índices admitidos en Amazon DocumentDB.

Introducción

Para iniciar la creación de índices en una colección, utilice el comando `createIndexes`. De forma predeterminada, el comando ejecutará dos elementos de trabajo paralelos, lo que aumentará dos veces la velocidad del proceso de creación del índice.

Por ejemplo, el siguiente proceso de comando muestra cómo crear un índice para el campo “user_name” de un documento y cómo aumentar la velocidad del proceso de indexación a cuatro elementos de trabajo:

1. Cree índices utilizando dos elementos de trabajo paralelos en el clúster:

```
db.runCommand({"createIndexes":"test","indexes":[{"key": {"user_name":1},
 "name":"username_idx"}]})
```

2. Para optimizar la velocidad del proceso de creación del índice, puede especificar el número de procesos de trabajo mediante la opción “subprocesos de trabajo” (`"workers":<number>`) del comando `db.runCommand createIndexes`.

   Aumente la velocidad del proceso a cuatro procesos de trabajo paralelos:

   ```
   db.runCommand({"createIndexes":"test","indexes":[{"key": {"user_name":1},
    "name":"username_idx", "workers":4}]})
   ```

   > **Note**
   >
   > Cuanto mayor sea el número de procesos de trabajo, más rápido avanzará la creación del índice. Sin embargo, cuanto mayor sea el número de trabajadores, mayor será la carga en las E/S de lectura CPUs y v de la instancia principal. Asegúrese de que el clúster esté lo suficientemente aprovisionado para soportar el aumento de la carga sin degradar otras cargas de trabajo.

Estado del progreso de indexación

El proceso de creación de índices funciona inicializando, escaneando las colecciones, clasificando las claves y, finalmente, insertándolas mediante un generador de índices. El proceso tiene hasta seis etapas cuando se ejecuta en primer plano y hasta nueve etapas cuando se ejecuta en segundo plano. Puede ver las métricas de estado, como el porcentaje de finalización, el número total de bloques de almacenamiento escaneados, las claves clasificadas y las claves insertadas, etapa por etapa.

Supervise el progreso del proceso de indexación mediante el comando `db.currentOp()` del shell mongo. Una finalización del 100 % de la última etapa indica que todos los índices se han creado correctamente:

```
db.currentOp({"command.createIndexes": { $exists : true } })
```

> **Note**
>
> La visualización del estado del progreso de la indexación se admite solamente en Amazon DocumentDB 5.0.

Tipos de creación de índices

Los cuatro tipos de compilaciones de índices son:

- Primer plano: la compilación del índice en primer plano bloquea todas las demás operaciones de la base de datos hasta que se crea el índice. La compilación en primer plano de Amazon DocumentDB consta de cinco etapas.
- Primer plano (único): las compilaciones de índices en primer plano de un solo documento (únicas) bloquean otras operaciones de la base de datos como las compilaciones en primer plano normales. A diferencia de la compilación básica en primer plano, la compilación única utiliza una etapa adicional (clasificación de claves 2) para buscar claves duplicadas. La compilación en primer plano (única) consta de seis etapas.
- Fondo: la compilación del índice en segundo plano permite que otras operaciones de la base de datos se ejecuten en primer plano mientras se crea el índice. La compilación de fondo de Amazon DocumentDB consta de ocho etapas.
- Fondo (único): las compilaciones de índices en segundo plano de un solo documento (único) permiten que otras operaciones de la base de datos se ejecuten en primer plano mientras se crea el índice. A diferencia de la compilación básica de fondo, la compilación única utiliza una etapa adicional (clasificación de claves 2) para buscar claves duplicadas. La compilación de fondo (única) se compone de nueve etapas.

Etapas de compilación del índice

Etapa	Primer plano	Primer plano (único)	Introducción	Fondo (único)
Inicializando	1	1	1	1
creando índice: inicializando	2	2	2	2.
creando índice: escaneando colección	3	3	3	3

Etapa	Primer plano	Primer plano (único)	Introducción	Fondo (único)
creando índice: clasificando claves 1	4	4	4	4
creando índice: clasificando claves 2		5		5
creando índice: insertando claves	5	6	5	6
validando: escaneando índice			6	7
validando: clasificando tuplas			7	8
validando: escaneando colección			8	9

- inicializando: createIndex está preparando el generador de índices. Esta fase debe ser muy breve.
- creando índice: inicializando: el generador de índices se está preparando para crear el índice. Esta fase debe ser muy breve.
- creando índice: escaneando colección: el generador de índices está escaneando la colección para recopilar las claves del índice. La unidad de medida son los “bloques”.

> **Note**
>
> Si hay más de un elemento de trabajo configurado para la compilación del índice, se mostrará en esta etapa. La etapa “escaneando colección” es la única etapa en la que se

utilizan varios procesos de trabajo durante el proceso de compilación del índice. En todas las demás etapas se mostrará un único proceso de trabajo.

- creando índice: clasificando claves 1: el generador de índices está clasificando las claves de índice recopiladas. La unidad de medida son las “claves”.
- creando índice: clasificando claves 2: el generador de índices está clasificando las claves de índice recopiladas que corresponden a tuplas muertas. Esta fase solo existe para la compilación de índices únicos. La unidad de medida son las “claves”.
- creando índice: insertando claves: el generador de índices está insertando claves de índice en el nuevo índice. La unidad de medida son las “claves”.
- validando: escaneando índice: createIndex está escaneando el índice para buscar las claves que deben validarse. La unidad de medida son los “bloques”.
- validando: clasificando tuplas: createIndex está ordenando el resultado de la fase de escaneo del índice.
- validando: escaneando colección: createIndex está escaneando la colección para validar las claves de índice encontradas en las dos fases anteriores. La unidad de medida son los “bloques”.

Ejemplo de salida de compilación del índice

En el siguiente ejemplo de salida (compilación del índice en primer plano), se muestra el estado de la creación del índice. El campo “msg” resume el progreso de la compilación indicando la etapa y el porcentaje de finalización de la compilación. El campo “procesos de trabajo” indica el número de procesos de trabajo utilizados durante esa etapa de la compilación del índice. El campo “progreso” muestra los números reales utilizados para calcular el porcentaje de finalización.

Note

Los campos «currentIndexBuildNombre», «mensaje» y «progreso» no son compatibles con la versión 4.0 de Amazon DocumentDB.

```
{
    "inprog" : [{
    …
        "command": {
            "createIndexes": "test",
            "indexes": [{
```

```
                "v": 2,
                "key": {
                    "user_name": 1
                },
                "name": "user_name_1"
            }],
            "lsid": {
                "id": UUID("094d0fba-8f41-4373-82c3-7c4c7b5ff13b")
            },
            "$db": "test"
        },
        "currentIndexBuildName": user_name_1,
        "msg": "Index Build: building index number_1, stage 6/6 building index:
 656860/1003520 (keys) 65%",
        "workers": 1,
        "progress": {
            "done": 656861,
            "total": 1003520
        },
    …
    ],

    "ok" : 1
}
```

Mantenimiento de índices de Amazon DocumentDB

Temas

- Sobrecarga del índice
- Mantenimiento de índices mediante reIndex

Sobrecarga del índice

Amazon DocumentDB utiliza el control de concurrencia multiversión (MVCC) para gestionar las transacciones simultáneas. Cuando los documentos se eliminan o actualizan, sus versiones anteriores permanecen en las colecciones e índices como versiones «inactivas». El proceso de recopilación de elementos no utilizados recupera automáticamente el espacio de estas versiones inactivas para futuras operaciones.

La sobrecarga de índices se produce cuando el tamaño de los índices de una colección aumenta debido a la acumulación de índices inactivos u obsoletos o a la fragmentación de las páginas. El

porcentaje informado representa la cantidad de espacio de índice que pueden utilizar las entradas de índice futuras. Esta sobrecarga consume espacio tanto en la memoria caché como en el almacenamiento del búfer. Si desea eliminar la sobrecarga, tendrá que recopilar los índices.

Example Ejemplo

Ejecute el siguiente comando para determinar el almacenamiento no utilizado del índice:

```
db.coll.aggregate({$indexStats:{}});
```

El resultado tendrá un aspecto parecido al siguiente:

```
{
    "name" : "_id_",
    "key" : {
        "_id" : 1
    },
    "host" : "devbox-test.localhost.a2z.com:27317",
    "size" : NumberLong(827392),
    "accesses" : {
        "ops" : NumberLong(40000),
        "docsRead" : NumberLong(46049),
        "since" : ISODate("2025-04-03T21:44:51.251Z")
    },
    "cacheStats" : {
        "blksRead" : NumberLong(264),
        "blksHit" : NumberLong(140190),
        "hitRatio" : 99.8121
    },
    "unusedStorageSize" : {
        "unusedSizeBytes" : 409600,
        "unusedSizePercent" : 49.51
    }
}
```

Puede reconstruir los índices sin tiempo de inactividad mediante el comando `reIndex`, que requiere escanear toda la colección. Consulte Mantenimiento de índices mediante `reIndex`.

Mantenimiento de índices mediante **`reIndex`**

`reIndex` es un comando que se utiliza para reconstruir un índice. Se utiliza normalmente cuando un índice está dañado o es ineficiente. Con el tiempo, los índices pueden acumular espacio no utilizado

debido a muchas actualizaciones, inserciones o eliminaciones, lo que reduce el rendimiento. La reindexación ayuda a eliminar ese espacio no utilizado y a restablecer la eficiencia del índice.

Directrices de **`reIndex`**

- `reIndex` solo es compatible con Amazon DocumentDB 5.0.
- Amazon DocumentDB admite `reindex` un único índice en segundo plano, lo que permite varios procesos de trabajo. Las consultas pueden utilizar el índice anterior cuando el proceso de `reIndex` está en ejecución.
- Amazon DocumentDB admite informes de progreso de indexación a través de `currentOp`. Puede ver las etapas de creación del índice de forma similar a las Etapas de compilación del índice vistas durante la creación del índice. La única diferencia es que `reIndex` siempre tiene ocho etapas, independientemente de si son únicas o no. No existe una etapa de “creación de índices: claves de clasificación 2”.
- `reIndex` se puede ejecutar simultáneamente con cualquier comando, excepto los comandos relacionados con índices de la misma colección: `createIndexes`, `dropIndexes`, `collMod` y `renameCollection`.
- `reIndex` actualmente no es compatible con índices de texto, geoespaciales, vectoriales ni parciales.

Creación de **`reIndex`**

Use el siguiente comando para reconstruir el índice:

```
db.runCommand({ reIndex: "collection-name", index: "index-name"})
```

Si lo desea, también puede controlar el número de procesos de trabajo asignados al proceso de reconstrucción:

```
db.runCommand({ reIndex: "collection-name", index: "index-name", workers: number })
```

Gestión de la compresión de documentos a nivel de colección

La compresión de documentos a nivel de colección de Amazon DocumentDB 5.0 le permite reducir los costos de almacenamiento y E/S al comprimir los documentos de sus colecciones. Puede habilitar la compresión de documentos a nivel de colección y ver las métricas de compresión según

sea necesario, midiendo las ganancias de almacenamiento mediante métricas de compresión como es el tamaño de almacenamiento de los documentos comprimidos y el estado de la compresión. Amazon DocumentDB 5.0 utiliza el algoritmo de LZ4 compresión para comprimir documentos.

Amazon DocumentDB admite la compresión de documentos a partir de la versión 5.0. Las siguientes son funciones de compresión de documentos a nivel de colección:

- Comportamiento predeterminado: la configuración de compresión predeterminada para las nuevas colecciones de un clúster de la versión 5.0 viene determinada por el parámetro `default_collection_compression` del clúster. Este parámetro está establecido en "deshabilitado" de forma predeterminada.
- Compresión de las colecciones existentes: la configuración de compresión de las colecciones existentes se puede cambiar mediante el comando `collMod`.
- Cambio del umbral de compresión: el umbral de compresión predeterminado es de 2 KB. Este valor se puede especificar para las colecciones nuevas mediante el comando `createCollection` y se puede cambiar para las colecciones existentes mediante el comando `collMod`.

> **Note**
>
> La compresión de documentos de Amazon DocumentDB no es compatible en las versiones 3.6 y 4.0 de Amazon DocumentDB.

Temas

- Administración de la compresión de documentos
- Supervisión de la compresión de documentos

Administración de la compresión de documentos

Habilitación de la compresión de documentos en una colección

Active la compresión de documentos al crear una colección en Amazon DocumentDB 5.0 mediante `db.createCollection()` el método:

```
db.createCollection( sample_collection,{
```

```
    storageEngine : {
        documentDB: {
            compression:{enable: <true | false>}
        }
    }
})
```

Habilitación de la compresión de documentos en un clúster

La compresión de documentos se puede habilitar de forma predeterminada para todas las colecciones nuevas a nivel de clúster al establecer el parámetro `default_collection_compression` del clúster en “habilitado”. Si este parámetro se establece en “habilitado”, las colecciones recién creadas en el clúster tendrán la compresión habilitada de forma predeterminada con un umbral de compresión de 2 KB.

Compresión de colecciones existentes

También puede modificar la configuración de compresión de una colección existente mediante la operación `collMod` y especificando la siguiente configuración `storageEngine`. Tenga en cuenta que el cambio realizado con este comando solo se aplicará a inserted/updated los documentos nuevos y la compresión de los documentos insertados anteriormente no cambiará.

```
db.runCommand({
    collMod: "orders",
    storageEngine: {
        documentDB: {compression: {enable: <true | false>} }
    }
})
```

Establecimiento de los umbrales de compresión

De forma predeterminada, el umbral de compresión de las colecciones comprimidas es de 2032 bytes. Este valor de umbral se puede establecer en el comando `createCollection` al crear una nueva colección con la compresión habilitada:

```
db.createCollection( sample_collection, {
    storageEngine : {
        documentDB: {
            compression: {
                enable: true,
```

```
                threshold: <128 - 8000>
            }
        }
    }
})
```

También puede modificar el umbral de compresión de una colección comprimida existente mediante la operación `collMod` y al especificar la siguiente configuración `storageEngine`:

```
db.runCommand({
    collMod: "orders",
    storageEngine: {
        documentDB: {
            compression: {
                enable: true,
                threshold: <128 - 8000>
            }
        }
    }
})
```

Tenga en cuenta que el umbral de compresión solo se puede establecer en un valor entre 128 y 8000 bytes. Además, la opción `enable` debe estar configurada en “true” al especificar el umbral de compresión.

Supervisión de la compresión de documentos

Puede comprobar si una colección está comprimida y calcular la relación de compresión de la siguiente manera:

Para ver las estadísticas de compresión, ejecute el comando `db.printCollectionStats()` o `db.collection.stats()` desde el intérprete de comandos de mongo. El resultado muestra el tamaño original y el tamaño comprimido, que puede comparar para analizar las ganancias de almacenamiento derivadas de la compresión de documentos. En este ejemplo, se muestran las estadísticas de una colección denominada “sample_collection” a continuación. A continuación, se utiliza un factor de escala de 1024*1024 para generar los valores `size` y `storageSize` en MB.

```
db.sample_collection.stats(1024*1024)
```

El siguiente es un ejemplo del resultado para el comando anterior:

```
{
    "ns" : "test.sample_collection",
    "count" : 1000000,
    "size" : 3906.3,
    "avgObjSize" : 4096,
    "storageSize" : 1953.1,
    compression:{"enabled" : true,"threshold" : 2032},
    ...
}
```

- tamaño: el tamaño original de la colección de documentos.
- avgObjSize- El tamaño medio del documento antes de la compresión se redondea al primer decimal. La unidad de medida son bytes.
- StorageSize: el tamaño de almacenamiento de la colección después de la compresión. La unidad de medida son bytes.
- habilitada: indica si la compresión está habilitada o deshabilitada.

Para calcular la relación de compresión real, divida el tamaño de la colección entre el tamaño de almacenamiento (Size/StorageSize). En el ejemplo anterior, el cálculo es 3906.3/1953.1, lo que se traduce en una relación de compresión de 2:1.

Administración de la compresión basada en diccionarios en Amazon DocumentDB 8.0

Amazon DocumentDB 8.0 presenta un nuevo algoritmo de compresión de documentos, zstd, como una alternativa mejorada a. LZ4 Al habilitar la compresión de diccionarios en una colección de Amazon DocumentDB 8.0 seleccionando Zstd como algoritmo de compresión, los documentos de la colección se muestrean para crear un diccionario de compresión personalizado. Los documentos nuevos y actualizados se comprimen con este diccionario y el algoritmo zstd. Este enfoque suele lograr relaciones de compresión más altas que los métodos de compresión estándar, especialmente para colecciones con esquemas de documentos consistentes o nombres de campo repetidos.

Lz4 es un algoritmo diseñado para una compresión y descompresión rápidas. Se sabe que es liviano para la CPU y, al mismo tiempo, logra una compresión notable. Zstd es un algoritmo de uso general que, con la configuración predeterminada, usa más CPU pero logra mejores relaciones de compresión que lz4. El uso de diccionarios mejora aún más la compresión en la mayoría de los documentos JSON. Algunas de las ventajas del algoritmo Zstd son:

- Reducción de los costes de almacenamiento: unas relaciones de compresión más altas implican un menor uso del almacenamiento y unos costes más bajos.
- Menor rendimientoI/O: Compressed documents require less I/O, lo que podría mejorar.
- Optimizado para su colección: el diccionario está diseñado específicamente para los patrones de datos de su colección.

> **Note**
>
> La compresión basada en diccionarios no se admite en las versiones 3.6, 4.0 y 5.0 de Amazon DocumentDB.

Consideraciones sobre el rendimiento

La compresión Zstd implica las siguientes ventajas y desventajas:

- Almacenamiento frente a CPU: la compresión Zstd logra mejores relaciones de compresión, pero puede consumir un poco más de recursos de la CPU en comparación con la compresión. LZ4
- Compresión inicial: es posible que las nuevas colecciones no logren una compresión óptima hasta que no se hayan insertado suficientes documentos para formar un diccionario eficaz. En la actualidad, un diccionario se entrena si reúne al menos 100 documentos.
- Tipo de carga de trabajo: las cargas de trabajo de lectura intensiva en las que todos los datos caben en la caché del búfer pueden experimentar un aumento de la latencia y el uso de la CPU debido a la sobrecarga de descompresión.

La compresión Zstd es especialmente eficaz para colecciones con documentos pequeños, matrices de documentos y nombres de campos repetidos.

Habilitar la compresión basada en diccionarios

En el caso de colecciones nuevas, puede utilizar el siguiente comando para activar la compresión Zstd:

```
db.createCollection("myCollection",
    {
        storageEngine: {
```

```
            documentDB: {
                compression: {
                    enable: true,
                    algorithm: "zstd"
                }
            }
        }
    }
)
```

También puedes activar o modificar la compresión en una colección existente:

```
db.runCommand({
    collMod: "myCollection",
    storageEngine: {
        documentDB: {
            compression: {
                enable: true,
                algorithm: "zstd"
            }
        }
    }
})
```

Para habilitar el algoritmo Zstd en todas las colecciones del clúster, puede modificar el grupo de parámetros del clúster para seleccionar «zstd» como valor para el parámetro «default_collection_compression».

Introducción

Amazon DocumentDB 8.0 incluye la compresión Zstd activada de forma predeterminada. Siempre puede desactivarla configurando el valor de 'default_compression' como deshabilitado en el grupo de parámetros del clúster. Debe tenerse en cuenta que, a partir de Amazon DocumentDB 8.0, «activado» ya no es una opción válida para default_compression y debe seleccionar entre Zstd y. LZ4

Supervisión

Puede ver la información de compresión de una colección mediante uno de los siguientes comandos:

- db.runCommand ({CollStats: «myCollection»}) O
- db.collection.stats ()

Estos comandos devuelven estadísticas clave que puede utilizar para calcular la relación de compresión:

- algoritmo de compresión: el algoritmo utilizado («lz4" o «zstd»)
- StorageSize: el almacenamiento real que utiliza la colección después de la compresión. Tenga en cuenta que este número incluye la fragmentación (es decir, el espacio no utilizado en las páginas de la base de datos)
- avgObjSize: El tamaño lógico promedio de los documentos de la colección, descomprimido. Tenga en cuenta que si su colección tiene más de 20 000 documentos, este número será una aproximación basada en una muestra de 20 000 documentos.
- tamaño: el tamaño lógico de la colección sin compresión. Este número se obtiene multiplicando avgObjSize por el número total de documentos de la colección, por lo que si avgObjSize es una aproximación, este número también será una aproximación.
- recuento: número de documentos de la colección

Las siguientes CloudWatch métricas pueden resultar útiles a la hora de evaluar la compresión basada en diccionarios:

- CPUUtilization
- FreeableMemory
- VolumeBytesUsed
- VolumeReadIOPs
- VolumeWriteIOPs

Métricas de CollStats:

- storageSize
- tamaño

Además, puede resultar útil realizar un seguimiento de las métricas específicas de la aplicación, como la latencia y el rendimiento por tipo de consulta o API.

Administración de eventos de Amazon DocumentDB

Amazon DocumentDB (con compatibilidad con MongoDB) mantiene un registro de los eventos relacionados con los clústeres, las instancias, las instantáneas, los grupos de seguridad y los grupos de parámetros de clúster. Esta información incluye la fecha y hora del evento, el nombre del origen y el tipo del origen del evento y un mensaje relacionado con el evento.

> **Important**
>
> En determinadas características de administración, Amazon DocumentDB utiliza una tecnología operativa que comparte con Amazon RDS y Amazon Neptune. Los límites regionales, es decir, los límites que se aplican en el nivel de región, se comparten entre Amazon DocumentDB, Amazon RDS, y Amazon Neptune. Para obtener más información, consulte Cuotas regionales.

Temas

- Visualización de las categorías de eventos de Amazon DocumentDB
- Visualización de eventos de Amazon DocumentDB

Visualización de las categorías de eventos de Amazon DocumentDB

Cada tipo de recurso de Amazon DocumentDB, tiene tipos específicos de eventos que se pueden asociar a él. Puede utilizar la operación `describe-event-categories` de la AWS CLI para ver la correspondencia entre los tipos de eventos y los tipos de recursos de Amazon DocumentDB.

Parámetros

- **`--source-type`**: opcional. Utilice el parámetro `--source-type` para ver las categorías de eventos de un tipo de origen particular. Se permiten los siguientes valores:
  - `db-cluster`
  - `db-instance`
  - `db-parameter-group`
  - `db-security-group`
  - `db-cluster-snapshot`

- **`--filters`**: opcional. Para ver categorías de eventos únicamente para Amazon DocumentDB, utilice el filtro `--filter Name=engine,Values=docdb`.

Example

El siguiente código muestra las categorías de eventos asociadas a los clústeres.

Para Linux, macOS o Unix:

```
aws docdb describe-event-categories \
    --filter Name=engine,Values=docdb \
    --source-type db-cluster
```

Para Windows:

```
aws docdb describe-event-categories ^
    --filter Name=engine,Values=docdb ^
    --source-type db-cluster
```

La salida de esta operación será similar a lo que se indica a continuación (formato JSON).

```
{
    "EventCategoriesMapList": [
        {
            "EventCategories": [
                "notification",
                "failure",
                "maintenance",
                "failover"
            ],
            "SourceType": "db-cluster"
        }
    ]
}
```

El siguiente código muestra las categorías de eventos asociadas a cada tipo de recurso de Amazon DocumentDB.

```
aws docdb describe-event-categories
```

La salida de esta operación será similar a lo que se indica a continuación (formato JSON).

```
{
    "EventCategoriesMapList": [
        {
            "SourceType": "db-instance",
            "EventCategories": [
                "notification",
                "failure",
                "creation",
                "maintenance",
                "deletion",
                "recovery",
                "restoration",
                "configuration change",
                "read replica",
                "backtrack",
                "low storage",
                "backup",
                "availability",
                "failover"
            ]
        },
        {
            "SourceType": "db-security-group",
            "EventCategories": [
                "configuration change",
                "failure"
            ]
        },
        {
            "SourceType": "db-parameter-group",
            "EventCategories": [
                "configuration change"
            ]
        },
        {
            "SourceType": "db-cluster",
            "EventCategories": [
                "notification",
                "failure",
                "maintenance",
                "failover"
            ]
```

```
        },
        {
            "SourceType": "db-cluster-snapshot",
            "EventCategories": [
                "backup"
            ]
        }
    ]
}
```

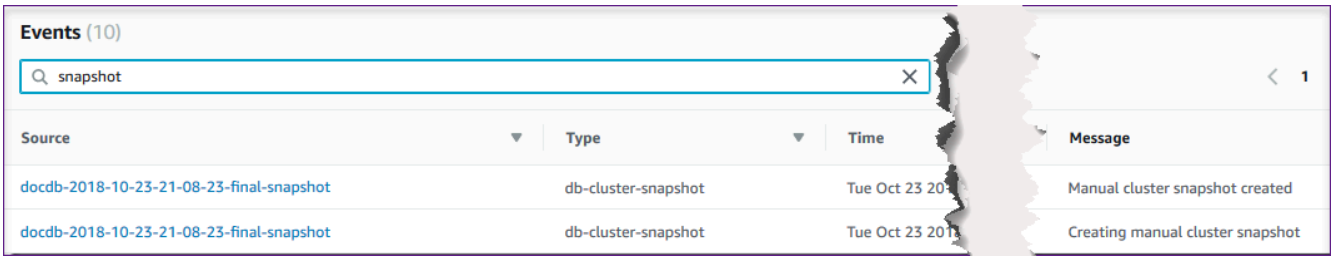
Visualización de eventos de Amazon DocumentDB

Puede recuperar eventos de los recursos de Amazon DocumentDB a través de la consola de Amazon DocumentDB, la cual muestra los eventos de las últimas 24 horas. También puede recuperar eventos para los recursos de Amazon DocumentDB utilizando el comando describe-events AWS CLI, o la operación DescribeEvents de la API de Amazon DocumentDB. Si utiliza la AWS CLI o la API de Amazon DocumentDB para ver eventos, puede recuperar eventos de los últimos 14 días como máximo.

Using the Consola de administración de AWS

Visualización de todos los eventos de las instancias de Amazon DocumentDB de las últimas 24 horas

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon DocumentDB en https://console.aws.amazon.com/docdb.
2. En el panel de navegación, seleccione Events. Los eventos disponibles aparecen en una lista.
3. Utilice la lista Filter (Filtro) para filtrar los eventos por tipo. Escriba un término en el cuadro de texto para filtrar aún más los resultados. Por ejemplo, la siguiente captura de pantalla muestra la filtración de todos los eventos de Amazon DocumentDB para los eventos de instantánea.



Using the AWS CLI

Visualización de todos los eventos de las instancias de Amazon DocumentDB de los últimos 7 días

Puede ver todos los eventos de las instancias de Amazon DocumentDB de los últimos 7 días ejecutando la operación describe-events de la AWS CLI con el parámetro `--duration` establecido en `10080` (10 080 minutos).

```
aws docdb describe-events --duration 10080
```

Filtrado de eventos de Amazon DocumentDB

Para ver eventos de Amazon DocumentDB específicos, utilice la operación `describe-events` con los siguientes parámetros.

Parámetros

- **`--filter`**: necesario para limitar los valores devueltos a los eventos de Amazon DocumentDB. Utilice **`Name=engine,Values=docdb`** para filtrar todos los eventos únicamente para Amazon DocumentDB.
- **`--source-identifier`**: opcional. El identificador del origen de eventos para el que se devuelven eventos. Si se omite, se incluyen en los resultados los eventos de todos los orígenes.
- **`--source-type`**: opcional, a menos que se proporcione `--source-identifier`, entonces es obligatorio. Si se proporciona `--source-identifier`, `--source-type` debe coincidir con el tipo de `--source-identifier`. Se permiten los siguientes valores:
  - `db-cluster`
  - `db-instance`
  - `db-parameter-group`
  - `db-security-group`
  - `db-cluster-snapshot`

El siguiente ejemplo muestra todos los eventos de Amazon DocumentDB.

```
aws docdb describe-events --filters Name=engine,Values=docdb
```

La salida de esta operación será similar a lo que se indica a continuación (formato JSON).

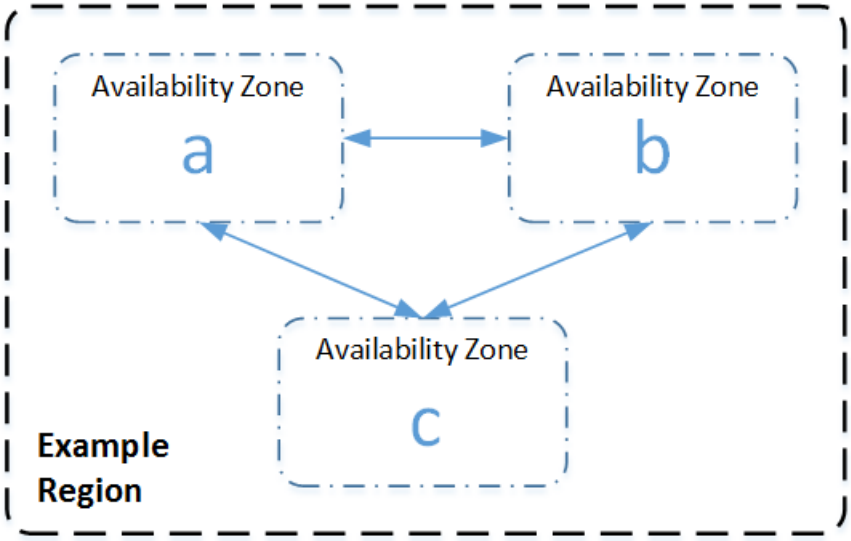
```
{
    "Events": [
        {
            "SourceArn": "arn:aws:rds:us-east-1:123SAMPLE012:db:sample-cluster-
instance3",
            "Message": "instance created",
            "SourceType": "db-instance",
            "Date": "2018-12-11T21:17:40.023Z",
            "SourceIdentifier": "sample-cluster-instance3",
            "EventCategories": [
                "creation"
            ]
        },
        {
            "SourceArn": "arn:aws:rds:us-
east-1:123SAMPLE012:db:docdb-2018-12-11-21-08-23",
            "Message": "instance shutdown",
            "SourceType": "db-instance",
            "Date": "2018-12-11T21:25:01.245Z",
            "SourceIdentifier": "docdb-2018-12-11-21-08-23",
            "EventCategories": [
                "availability"
            ]
        },
        {
            "SourceArn": "arn:aws:rds:us-
east-1:123SAMPLE012:db:docdb-2018-12-11-21-08-23",
            "Message": "instance restarted",
            "SourceType": "db-instance",
            "Date": "2018-12-11T21:25:11.441Z",
            "SourceIdentifier": "docdb-2018-12-11-21-08-23",
            "EventCategories": [
                "availability"
            ]
        }
    ]
}
```

Para obtener más información, consulte Auditoría de eventos de Amazon DocumentDB.

Elección de regiones y zonas de disponibilidad

Los recursos de computación en la nube de Amazon están alojados en varias ubicaciones de todo el mundo. Estas ubicaciones constan Regiones de AWS de zonas de disponibilidad. Cada Región de AWS es un área geográfica independiente. Cada región tiene varias ubicaciones aisladas conocidas como zonas de disponibilidad. Amazon DocumentDB le ofrece la posibilidad de colocar recursos, como instancias, y datos en varias ubicaciones. Los recursos no se replican en todos los demás, Regiones de AWS a menos que lo haga específicamente.

Amazon opera centros de datos de alta disponibilidad con tecnología de vanguardia. Aunque es infrecuente, puede suceder que se produzcan errores que afecten a la disponibilidad de las instancias que están en la misma ubicación. Si hospeda todas las instancias en una misma ubicación y se produce un error en ella, ninguna de las instancias estaría disponible. El siguiente diagrama muestra una Región de AWS con tres zonas de disponibilidad.



Es importante recordar que cada región es completamente independiente. Cualquier actividad de Amazon DocumentDB que se inicie (por ejemplo, la creación de instancias o la enumeración de las instancias de base de datos disponibles) se ejecuta solo en la Región de AWS predeterminada actual. Puede cambiar la región predeterminada en la consola configurando la variable de entorno `EC2_REGION`. También puede invalidarla mediante el parámetro `--region` de la AWS CLI. Para obtener más información, consulte Configurar AWS Command Line Interface, específicamente, las secciones sobre variables de entorno y opciones de línea de comandos.

Cuando crea un clúster mediante la consola de Amazon DocumentDB y decide crear una réplica en una zona de disponibilidad diferente, Amazon DocumentDB crea dos instancias. Crea la instancia

principal en una zona de disponibilidad y la instancia de réplica en una zona de disponibilidad diferente. El volumen del clúster siempre se replica en tres zonas de disponibilidad.

Para crear o trabajar con una instancia de Amazon DocumentDB en una instancia específica Región de AWS, utilice el punto de enlace de servicio regional correspondiente.

Disponibilidad por región

Amazon DocumentDB está disponible en las siguientes AWS regiones.

Regiones compatibles con Amazon DocumentDB

Nombre de la región	Region	Zonas de disponibilidad (cálculo)
Este de EE. UU. (Ohio)	`us-east-2`	3
Este de EE. UU. (Norte de Virginia)	`us-east-1`	6
Oeste de EE. UU. (Oregón)	`us-west-2`	4
África (Ciudad del Cabo)	`af-south-1`	3
América del Sur (São Paulo)	`sa-east-1`	3
Asia-Pacífico (Hong Kong)	`ap-east-1`	3
Asia-Pacífico (Hyderabad)	`ap-south-2`	3
Asia-Pacífico (Malasia)	`ap-southeast-5`	3
Asia-Pacífico (Mumbai)	`ap-south-1`	3

Nombre de la región	Region	Zonas de disponibilidad (cálculo)
Asia-Pacífico (Osaka)	ap-northeast-3	3
Asia-Pacífico (Seúl)	ap-northeast-2	4
Asia-Pacífico (Singapur)	ap-southeast-1	3
Asia-Pacífico (Sídney)	ap-southeast-2	3
Asia-Pacífico (Yakarta)	ap-southeast-3	3
Asia-Pacífico (Tailandia)	ap-southeast-7	3
Asia-Pacífico (Tokio)	ap-northeast-1	3
Canadá (centro)	ca-central-1	3
Región China (Pekín)	cn-north-1	3
China (Ningxia)	cn-northwest-1	3
Europa (Fráncfort)	eu-central-1	3
Europa (Irlanda)	eu-west-1	3
Europa (Londres)	eu-west-2	3
Europa (Milán)	eu-south-1	3
Europa (París)	eu-west-3	3
Europa (España)	eu-south-2	3
Europa (Estocolmo)	eu-north-1	3
México (centro)	mx-central-1	3

Nombre de la región	Region	Zonas de disponibilidad (cálculo)
Medio Oriente (EAU)	`me-central-1`	3
Israel (Tel Aviv)	`il-central-1`	3
AWS GovCloud (EE. UU.-Oeste)	`us-gov-west-1`	3
AWS GovCloud (EE. UU.-Este)	`us-gov-east-1`	3

Por defecto, la zona horaria de un clúster de Amazon DocumentDB es la hora universal coordinada (UTC).

Para obtener más información sobre cómo buscar puntos de conexión de clústeres e instancias en una región determinada, consulte Descripción de los puntos de conexión de Amazon DocumentDB.

Administración de los grupos de parámetros de clúster de Amazon DocumentDB

Es posible administrar la configuración del motor de Amazon DocumentDB mediante los parámetros de un grupo de parámetros de clúster. Un grupo de parámetros de clúster es una colección de valores de configuración de Amazon DocumentDB que facilitan la administración de los parámetros de los clústeres de Amazon DocumentDB. Los grupos de parámetros de clúster actúan como un contenedor para los valores de configuración del motor que se aplican a todas las instancias del clúster.

En esta sección se describe cómo crear, ver y modificar grupos de parámetros de clúster. También muestra cómo se puede determinar qué grupo de parámetros de clúster está asociado a un clúster determinado.

Temas

- Descripción de los grupos de parámetros de clúster de Amazon DocumentDB
- Creación de grupos de parámetros de clúster de Amazon DocumentDB
- Modificación de grupos de parámetros de clúster de Amazon DocumentDB

- Modificación de clústeres de Amazon DocumentDB para utilizar grupos de parámetros de clúster personalizados
- Copia de grupos de parámetros de clúster de Amazon DocumentDB
- Restablecimiento de grupos de parámetros de clúster de Amazon DocumentDB
- Borrado de grupos de parámetros de clúster de Amazon DocumentDB
- Referencia de parámetros de clúster de Amazon DocumentDB

Descripción de los grupos de parámetros de clúster de Amazon DocumentDB

Un grupo de parámetros de clúster `default` se crea automáticamente al crear el primer clúster de Amazon DocumentDB en una nueva región o al utilizar un motor nuevo. Los clústeres siguientes que se creen en la misma región y tengan la misma versión de motor se crean con el grupo de parámetros de clúster `default`.

Temas

- Descripción de los detalles de un grupo de parámetros de clúster de Amazon DocumentDB
- Determinación del grupo de parámetros de un clúster de Amazon DocumentDB

Descripción de los detalles de un grupo de parámetros de clúster de Amazon DocumentDB

Para describir los detalles de un grupo de parámetros de clúster determinado, complete los siguientes pasos con Consola de administración de AWS o AWS Command Line Interface (AWS CLI).

Using the Consola de administración de AWS

1. Inicie sesión en y abra la Consola de administración de AWS consola de Amazon DocumentDB en https://console.aws.amazon.com /docdb.
2. En el panel de navegación, seleccione Grupos de parámetros.

> **Tip**
>
> Si no ve el panel de navegación del lado izquierdo de la pantalla, seleccione el icono de menú
> (≡)
> en la esquina superior izquierda de la página.

3. En el panel Cluster parameter groups (Grupos de parámetros de clúster), seleccione el nombre del grupo de parámetros cuyos detalles desee ver.
4. La página resultante muestra los parámetros del grupo de parámetros, la actividad reciente y las etiquetas.

   - En Cluster parameters (Parámetros de clúster), puede ver el nombre del parámetro, el valor actual, los valores permitidos, si el parámetro es modificable, su tipo de aplicación, tipo de datos y descripción. Puede modificar parámetros individuales seleccionando el parámetro y eligiendo Edit (Editar) en la sección Cluster parameters (Parámetros de clúster) . Para obtener más información, consulte Modificación de parámetros de clúster de Amazon DocumentDB.
   - En Recent events (Eventos recientes), puede ver los eventos más recientes de este grupo de parámetros. Puede filtrar estos eventos mediante la barra de búsqueda de esta sección. Para obtener más información, consulte Administración de eventos de Amazon DocumentDB.
   - En Tags (Etiquetas), puede ver las etiquetas que se encuentran en este grupo de parámetros de clúster. Puede agregar o quitar etiquetas seleccionando Edit (Editar) en la sección Tags (Etiquetas) . Para obtener más información, consulte Etiquetado de recursos de Amazon DocumentDB.

Using the AWS CLI

Puede usar el `describe-db-cluster-parameter-groups` AWS CLI comando para ver el nombre del recurso de Amazon (ARN), la familia, la descripción y el nombre de un único grupo de parámetros de clúster o de todos los grupos de parámetros de clúster que tiene para Amazon DocumentDB. También puede usar el `describe-db-cluster-parameters` AWS CLI comando para ver los parámetros y sus detalles dentro de un único grupo de parámetros de clúster.

- **`--describe-db-cluster-parameter-groups`**: para ver una lista de todos los grupos de parámetros de clúster y sus detalles.
  - **`--db-cluster-parameter-group-name`**: opcional. El nombre del grupo de parámetros de clúster que desea describir. Si se omite este parámetro, se describen todos los grupos de parámetros de clúster.
- **`--describe-db-cluster-parameters`**: para obtener una lista de los parámetros de un grupo de parámetros, junto con sus valores.
  - **`--db-cluster-parameter-group name`**: obligatorio. El nombre del grupo de parámetros de clúster que desea describir.

Example

El código siguiente enumera hasta 100 grupos de parámetros de clúster y su ARN, familia, descripción y nombre.

```
aws docdb describe-db-cluster-parameter-groups
```

La salida de esta operación será similar a lo que se indica a continuación (formato JSON).

```
{
          "DBClusterParameterGroups": [
              {
                  "DBClusterParameterGroupArn": "arn:aws:rds:us-
east-1:012345678912:cluster-pg:default.docdb4.0",
                  "DBParameterGroupFamily": "docdb4.0",
                  "Description": "Default cluster parameter group for docdb4.0",
                  "DBClusterParameterGroupName": "default.docdb4.0"
              },
              {
                  "DBClusterParameterGroupArn": "arn:aws:rds:us-
east-1:012345678912:cluster-pg:sample-parameter-group",
                  "DBParameterGroupFamily": "docdb4.0",
                  "Description": "Custom docdb4.0 parameter group",
                  "DBClusterParameterGroupName": "sample-parameter-group"
              }
          ]
}
```

Example

El código siguiente enumera el ARN, la familia, la descripción y el nombre de `sample-parameter-group`.

Para Linux, macOS o Unix:

```
aws docdb describe-db-cluster-parameter-groups \
          --db-cluster-parameter-group-name sample-parameter-group
```

Para Windows:

```
aws docdb describe-db-cluster-parameter-groups ^
          --db-cluster-parameter-group-name sample-parameter-group
```

La salida de esta operación será similar a lo que se indica a continuación (formato JSON).

```
{
          "DBClusterParameterGroups": [
              {
                  "DBClusterParameterGroupArn": "arn:aws:rds:us-
east-1:123456789012:cluster-pg:sample-parameter-group",
                  "Description": "Custom docdb4.0 parameter group",
                  "DBParameterGroupFamily": "docdb4.0",
                  "DBClusterParameterGroupName": "sample-parameter-group"
              }
          ]
}
```

Example

El código siguiente enumera los valores de los parámetros de `sample-parameter-group`.

Para Linux, macOS o Unix:

```
aws docdb describe-db-cluster-parameters \
    --db-cluster-parameter-group-name sample-parameter-group
```

Para Windows:

```
aws docdb describe-db-cluster-parameters ^
    --db-cluster-parameter-group-name sample-parameter-group
```

La salida de esta operación será similar a lo que se indica a continuación (formato JSON).

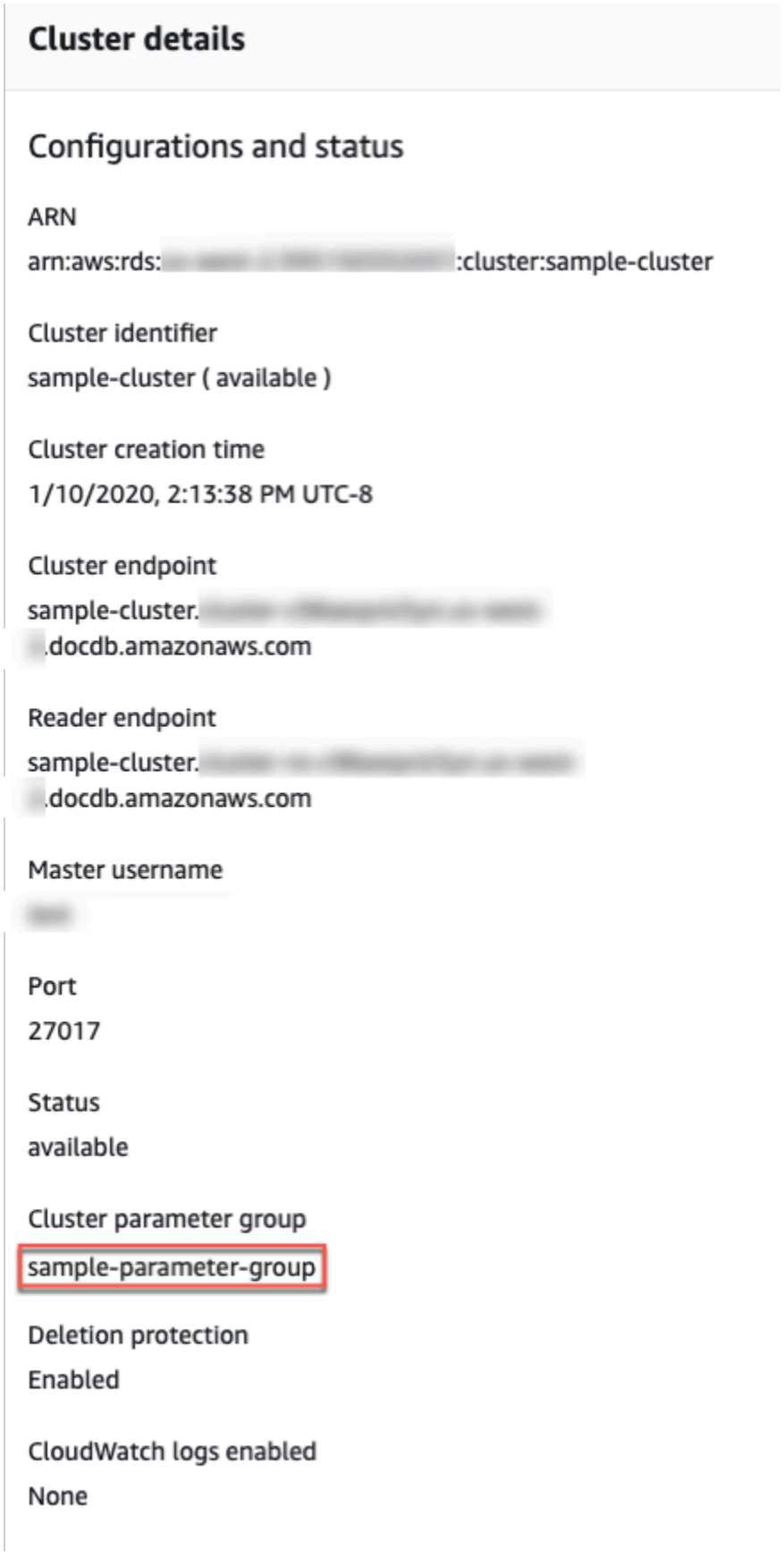
```
{
   "Parameters": [
         {
            "ParameterName": "audit_logs",
            "ParameterValue": "disabled",
            "Description": "Enables auditing on cluster.",
            "Source": "system",
            "ApplyType": "dynamic",
            "DataType": "string",
            "AllowedValues": "enabled,disabled",
            "IsModifiable": true,
            "ApplyMethod": "pending-reboot"
         },
         {
            "ParameterName": "change_stream_log_retention_duration",
            "ParameterValue": "17777",
            "Description": "Duration of time in seconds that the change stream log
 is retained and can be consumed.",
            "Source": "user",
            "ApplyType": "dynamic",
            "DataType": "integer",
            "AllowedValues": "3600-86400",
            "IsModifiable": true,
            "ApplyMethod": "pending-reboot"
         }
   ]
}
```

Determinación del grupo de parámetros de un clúster de Amazon DocumentDB

Para determinar qué grupo de parámetros está asociado a un clúster en particular, complete los siguientes pasos utilizando el Consola de administración de AWS o el AWS CLI.

Using the Consola de administración de AWS

1. Inicie sesión en y abra la Consola de administración de AWS consola de Amazon DocumentDB en https://console.aws.amazon.com /docdb.
2. En el panel de navegación izquierdo, elija Clusters (Clústeres).
3. En la lista de clústeres, elija el nombre del clúster de su interés.
4. La página resultante muestra los detalles del clúster seleccionado. Desplácese hacia abajo hasta Cluster details (Detalles del clúster). En la parte inferior de esa sección, busque el nombre del grupo de parámetros debajo del grupo de parámetros de clúster.


Cluster details
Configurations and status
ARN
arn:aws:rds: :cluster:sample-cluster
Cluster identifier
sample-cluster (available)
Cluster creation time
1/10/2020, 2:13:38 PM UTC-8
Cluster endpoint
sample-cluster.
.docdb.amazonaws.com
Reader endpoint
sample-cluster.
.docdb.amazonaws.com
Master username
Port
27017
Status
available
Cluster parameter group
sample-parameter-group
Deletion protection
Enabled
CloudWatch logs enabled
None

Using the AWS CLI

El siguiente AWS CLI código determina qué grupo de parámetros rige el clúster. `sample-cluster`

```
aws docdb describe-db-clusters \
      --db-cluster-identifier sample-cluster \
      --query 'DBClusters[*].[DBClusterIdentifier,DBClusterParameterGroup]'
```

La salida de esta operación será similar a lo que se indica a continuación (formato JSON).

```
[
       [
           "sample-cluster",
           "sample-parameter-group"
       ]
]
```

Creación de grupos de parámetros de clúster de Amazon DocumentDB

Los grupos de parámetros de clúster predeterminados como `default.docdb5.0`, `default.docdb4.0` o `default.docdb3.6`, se crean al crear un clúster con una nueva versión del motor y en una nueva región. Los clústeres siguientes que se creen en esta región y tengan la misma versión de motor heredan el grupo de parámetros de clúster `default`. Una vez creados, los grupos de parámetros `default` no se pueden eliminar ni cambiar de nombre. Puede modificar el comportamiento del motor de las instancias de clúster creando un grupo de parámetros personalizado con los valores de parámetros preferidos y adjuntándolo a su clúster de Amazon DocumentDB.

El siguiente procedimiento le guía a través de la creación de un grupo de parámetros de clúster personalizado. A continuación, puede modificar los parámetros dentro de ese grupo de parámetros.

> **Note**
>
> Después de crear un grupo de parámetros de clúster, debe esperar al menos 5 minutos antes de usar ese grupo de parámetros en concreto. Esto permite a `create` finalizar por completo la acción Amazon DocumentDB antes de que el grupo de parámetros de clúster se use para un nuevo clúster. Puede utilizar la `describe-db-cluster-parameter-groups` AWS CLI operación Consola de administración de AWS o para comprobar que se ha creado

el grupo de parámetros del clúster. Para obtener más información, consulte Descripción de los grupos de parámetros de clúster de Amazon DocumentDB.

Using the Consola de administración de AWS

Creación de un grupo de parámetros de clúster

1. Inicie sesión en y abra la Consola de administración de AWS consola de Amazon DocumentDB en https://console.aws.amazon.com /docdb.
2. En el panel de navegación, seleccione Grupos de parámetros.

   > **Tip**
   >
   > Si no ve el panel de navegación del lado izquierdo de la pantalla, seleccione el icono de menú
   > (≡)
   > en la esquina superior izquierda de la página.

3. En el panel Cluster parameter groups (Grupos de parámetros del clúster), elija Create (Crear).
4. En el panel Create cluster parameter group (Crear grupo de parámetros de clúster) escriba lo siguiente:

   a. Nombre del nuevo grupo de parámetros de clúster: escriba un nombre para el grupo de parámetros de clúster. Por ejemplo, `sample-parameter-group`. Los grupos de parámetros de clúster tienen las siguientes restricciones de denominación:

      - La longitud es de [1-255] caracteres alfanuméricos.
      - El primer carácter debe ser una letra.
      - No puede terminar con un guion ni contener dos guiones consecutivos.

   b. Familia: elija la versión de DocumentDB que desee usar para su clúster.

   c. Descripción: proporcione una descripción para este grupo de parámetros de clúster.

5. Para crear el grupo de parámetros de clúster, elija Create (Crear). Para cancelar la operación, elija Cancel (Cancelar).
6. Después de seleccionar Create (Crear), aparece el siguiente texto en la parte superior de la página para comprobar que el grupo de parámetros de clúster se ha creado correctamente:

```
Successfully created cluster parameter group 'sample-parameter-group'.
```

Using the AWS CLI

Para crear un nuevo grupo de parámetros de clúster para los clústeres de Amazon DocumentDB 4.0, utilice la AWS CLI `create-db-cluster-parameter-group` operación con los siguientes parámetros:

- **`--db-cluster-parameter-group-name`**: el nombre del grupo de parámetros de clúster de base de datos. Por ejemplo, `sample-parameter-group`.
- **`--db-cluster-parameter-group-family`**: la familia de grupos de parámetros de clúster que se utiliza como plantilla para el grupo de parámetros de clúster personalizado.
- **`--description`**: la descripción proporcionada por el usuario para este grupo de parámetros de clúster. El siguiente ejemplo utiliza "`Custom docdb4.0 parameter group`".

Para Linux, macOS o Unix:

Example

```
aws docdb create-db-cluster-parameter-group \
 --db-cluster-parameter-group-name sample-parameter-group \
 --db-parameter-group-family docdb5.0 \
 --description "Custom docdb5.0 parameter group"
```

Para Windows:

```
aws docdb create-db-cluster-parameter-group ^
 --db-cluster-parameter-group-name sample-parameter-group ^
 --db-parameter-group-family docdb5.0 ^
 --description "Custom docdb5.0 parameter group"
```

La salida de esta operación será similar a lo que se indica a continuación (formato JSON).

```
{
    "DBClusterParameterGroup": {
        "DBClusterParameterGroupName": "sample-parameter-group",
        "DBParameterGroupFamily": "docdb5.0",
```

```
        "Description": "Custom docdb4.0 parameter group",
        "DBClusterParameterGroupArn": "sample-parameter-group-arn"
    }
}
```

Modificación de grupos de parámetros de clúster de Amazon DocumentDB

En esta sección se explica cómo modificar un grupo de parámetros personalizados de Amazon DocumentDB. En Amazon DocumentDB, no puede modificar un grupo de parámetros de clúster `default` que se crea al crear por primera vez un clúster con una nueva versión del motor en una nueva región. Si el clúster de Amazon DocumentDB utiliza el grupo de parámetros de clúster predeterminado y desea modificar un valor en él, primero debe crear un nuevo grupo de parámetros o copiar un grupo de parámetros existente, modificarlo y, a continuación, aplicar el grupo de parámetros modificado a su clúster.

Siga los pasos siguientes para modificar un grupo de parámetros de clúster. Las acciones de modificación pueden tardar un tiempo en propagarse. Espere a que el grupo de parámetros de clúster modificado esté disponible antes de adjuntarlo al clúster. Puede utilizar la AWS CLI `describe-db-cluster-parameters` operación Consola de administración de AWS o para comprobar que el grupo de parámetros del clúster se ha modificado. Para obtener más información, consulte Descripción de los grupos de parámetros de clúster.

Using the Consola de administración de AWS

Siga estos pasos para modificar un grupo de parámetros personalizado de Amazon DocumentDB. No puede modificar un grupo de parámetros `default`. Si desea modificar un valor del grupo de parámetros `default`, puede copiar el grupo de parámetros del clúster por defecto, modificarlo y, a continuación, aplicar el grupo de parámetros modificado al clúster. Para obtener más información sobre la aplicación de grupos de parámetros al clúster, consulte Modificación de un clúster de Amazon DocumentDB.

Modificación de un grupo de parámetros de clúster personalizado

1. Inicie sesión en y abra la Consola de administración de AWS consola de Amazon DocumentDB en https://console.aws.amazon.com /docdb.
2. En el panel de navegación del lado izquierdo de la consola, elija Parameter groups (Grupos de parámetros). En la lista de grupos de parámetros, seleccione el nombre del grupo de parámetros que desee modificar.

> **Tip**
>
> Si no ve el panel de navegación del lado izquierdo de la pantalla, seleccione el icono de menú
> (≡)
> en la esquina superior izquierda de la página.

3. Para cada parámetro del grupo de parámetros que desee modificar, haga lo siguiente:

   a. Localice el parámetro que desea modificar y compruebe que es modificable comprobando si aparece en la `true` columna Modifiable (Modificable) .

   b. Si es modificable, seleccione el parámetro y elija Edit (Editar) en la parte superior derecha de la página de la consola.

   c. En el cuadro de diálogo Modify (Modificar) **<parameter-name>**, realice los cambios que desee. A continuación, elija Modify cluster parameter (Modificar el parámetro de clúster), o elija Cancel (Cancelar) para descartar los cambios.

Using the AWS CLI

Puede modificar los valores de `ParameterValue`, `Description` o `ApplyMethod` de cualquier parámetro modificable de un grupo de parámetros de clúster personalizado de Amazon DocumentDB mediante la AWS CLI. No se pueden realizar modificaciones directamente en un grupo de parámetros de clúster por defecto.

Para modificar los parámetros de un grupo de parámetros de clúster personalizado, utilice la operación `modify-db-cluster-parameter-group` con los siguientes parámetros.

- **`--db-cluster-parameter-group-name`**: obligatorio. El nombre del grupo de parámetros de clúster que va a modificar.
- **`--parameters`**: obligatorio. Los parámetros que está modificando. Para obtener una lista de los parámetros que se aplican a todas las instancias de un clúster de Amazon DocumentDB, consulte Referencia de parámetros de clúster de Amazon DocumentDB. Cada entrada de parámetro debe incluir lo siguiente:
  - **`ParameterName`**: el nombre del grupo de parámetros de clúster que va a modificar.
  - **`ParameterValue`**: el valor nuevo de este parámetro de clúster.

- **`ApplyMethod`**: cómo desea que se apliquen los cambios a este parámetro. Los valores permitidos son `immediate` y `pending-reboot`.

> **Note**
>
> Los parámetros con el `ApplyType` de `static` deben tener un `ApplyMethod` de `pending-reboot`.

Example - Modificación del valor de un parámetro

En este ejemplo, se muestran los valores de parámetro de `sample-parameter-group` y se modifica el parámetro `tls`. A continuación, después de 5 minutos, también se muestran los valores de parámetro de `sample-parameter-group` para ver los valores de parámetro que han cambiado.

1. Muestre los parámetros de `sample-parameter-group` y sus valores.

   Para Linux, macOS o Unix:

   ```
   aws docdb describe-db-cluster-parameters \
          --db-cluster-parameter-group-name sample-parameter-group
   ```

   Para Windows:

   ```
   aws docdb describe-db-cluster-parameters ^
          --db-cluster-parameter-group-name sample-parameter-group
   ```

   La salida de esta operación será similar a lo que se indica a continuación (formato JSON).

   ```
   {
          "Parameters": [
              {
                  "Source": "system",
                  "ApplyType": "static",
                  "AllowedValues": "disabled,enabled",
                  "ParameterValue": "enabled",
                  "ApplyMethod": "pending-reboot",
                  "DataType": "string",
                  "ParameterName": "tls",
   ```

```
                "IsModifiable": true,
                "Description": "Config to enable/disable TLS"
            },
            {
                "Source": "user",
                "ApplyType": "dynamic",
                "AllowedValues": "disabled,enabled",
                "ParameterValue": "enabled",
                "ApplyMethod": "pending-reboot",
                "DataType": "string",
                "ParameterName": "ttl_monitor",
                "IsModifiable": true,
                "Description": "Enables TTL Monitoring"
            }
        ]
}
```

2. Modifique el parámetro `tls` para que su valor sea `disabled`.

   No se puede modificar `ApplyMethod` ya que `ApplyType` es `static`.

   Para Linux, macOS o Unix:

```
aws docdb modify-db-cluster-parameter-group \
       --db-cluster-parameter-group-name sample-parameter-group \
       --parameters
 "ParameterName"=tls,"ParameterValue"=disabled,"ApplyMethod"=pending-reboot
```

   Para Windows:

```
aws docdb modify-db-cluster-parameter-group ^
       --db-cluster-parameter-group-name sample-parameter-group ^
       --parameters
 "ParameterName"=tls,"ParameterValue"=disabled,"ApplyMethod"=pending-reboot
```

   La salida de esta operación será similar a lo que se indica a continuación (formato JSON).

```
{
       "DBClusterParameterGroupName": "sample-parameter-group"
   }
```

3. Espere al menos 5 minutos.

4. Enumere los valores de parámetro de `sample-parameter-group` para verificar que se modificó el parámetro de `tls`.

   Para Linux, macOS o Unix:

   ```
   aws docdb describe-db-cluster-parameters \
          --db-cluster-parameter-group-name sample-parameter-group
   ```

   Para Windows:

   ```
   aws docdb describe-db-cluster-parameters ^
          --db-cluster-parameter-group-name sample-parameter-group
   ```

   La salida de esta operación será similar a lo que se indica a continuación (formato JSON).

   ```
   {
          "Parameters": [
              {
                  "ParameterValue": "false",
                  "ParameterName": "enable_audit_logs",
                  "ApplyType": "dynamic",
                  "DataType": "string",
                  "Description": "Enables auditing on cluster.",
                  "AllowedValues": "true,false",
                  "Source": "system",
                  "IsModifiable": true,
                  "ApplyMethod": "pending-reboot"
              },
              {
                  "ParameterValue": "disabled",
                  "ParameterName": "tls",
                  "ApplyType": "static",
                  "DataType": "string",
                  "Description": "Config to enable/disable TLS",
                  "AllowedValues": "disabled,enabled",
                  "Source": "system",
                  "IsModifiable": true,
                  "ApplyMethod": "pending-reboot"
              }
          ]
   }
   ```

Modificación de clústeres de Amazon DocumentDB para utilizar grupos de parámetros de clúster personalizados

Al crear un clúster de Amazon DocumentDB, se crea automáticamente un grupo de parámetros `default.docdb4.0` para ese clúster. No se puede modificar el grupo de parámetros del clúster `default`. En su lugar, puede modificar el clúster de Amazon DocumentDB para asociar un nuevo grupo de parámetros personalizados con él.

En esta sección se explica cómo modificar un clúster de Amazon DocumentDB existente para que utilice un grupo de parámetros de clúster personalizado con Consola de administración de AWS y AWS Command Line Interface ()AWS CLI.

Using the Consola de administración de AWS

Modificación de un clúster de Amazon DocumentDB para utilizar un nuevo grupo de parámetros de clúster no predeterminado

1. Antes de comenzar, asegúrese de haber creado un clúster de Amazon DocumentDB y un grupo de parámetros de clúster. Consulte Creación de un clúster de Amazon DocumentDB y Creación de grupos de parámetros de clúster de Amazon DocumentDB para obtener más instrucciones.
2. Después de crear el grupo de parámetros de clúster, abra la consola de Amazon DocumentDB en https://console.aws.amazon.com/docdb. En el panel de navegación, elija Clusters (Clústeres) para añadir el nuevo grupo de parámetros a un clúster.
3. Elija el clúster al que desea asociar el grupo de parámetros. Elija Actions (Acciones), y, a continuación, elija Modify (Modificar) para modificar el clúster.
4. En Cluster options (Opciones de clúster), elija el nuevo grupo de parámetros al que desea asociar el clúster.
5. Elija Continue (Continuar) para ver un resumen de las modificaciones.
6. Después de verificar los cambios, puede aplicarlos inmediatamente o durante el siguiente período de mantenimiento en Scheduling of modifications (Programación de modificaciones).
7. Elija Modify cluster (Modificar clúster) para actualizar el clúster con el nuevo grupo de parámetros.

Using the AWS CLI

Antes de comenzar, asegúrese de haber creado un clúster de Amazon DocumentDB y un grupo de parámetros de clúster. Puede crear un clúster de Amazon DocumentDB mediante la AWS CLI `create-db-cluster` operación. Puede crear un grupo de parámetros de clúster mediante la AWS CLI `create-db-cluster-parameter-group` operación.

Para añadir el nuevo grupo de parámetros del clúster al clúster, utilice la AWS CLI `modify-db-cluster` operación con los siguientes parámetros.

- -- db-cluster-identifier — El nombre del clúster (por ejemplo,`sample-cluster`).
- -- db-cluster-parameter-group -name: el nombre del grupo de parámetros al que desea asociar el clúster (por ejemplo,`sample-parameter-group`).

Example

```
aws docdb modify-db-cluster \
    --db-cluster-identifier sample-cluster \
    --db-cluster-parameter-group-name sample-parameter-group
```

La salida de esta operación será similar a lo que se indica a continuación (formato JSON).

```
"DBCluster": {
    "AvailabilityZones": [
            "us-west-2c",
            "us-west-2b",
            "us-west-2a"
    ],
    "BackupRetentionPeriod": 1,
    "DBClusterIdentifier": "sample-cluster",
    "DBClusterParameterGroup": "sample-parameter-group",
    "DBSubnetGroup": "default",
   ...
}
```

Copia de grupos de parámetros de clúster de Amazon DocumentDB

Puede hacer una copia de un grupo de parámetros de clúster en Amazon DocumentDB con Consola de administración de AWS o AWS Command Line Interface ()AWS CLI.

Using the Consola de administración de AWS

El siguiente procedimiento le guía a través de la creación de un nuevo grupo de parámetros de clúster mediante una copia de un grupo de parámetros de clúster existente.

Copiar de un grupo de parámetros de clúster

1. Inicie sesión en y abra la Consola de administración de AWS consola de Amazon DocumentDB en https://console.aws.amazon.com /docdb.
2. En el panel de navegación, seleccione Grupos de parámetros.
3. En el panel Cluster parameter groups (Grupos de parámetros del clúster), seleccione el nombre del grupo de parámetros de clúster que quiera copiar.
4. Elija Actions (Acciones), y, a continuación, elija Copy (Copiar) para copiar ese grupo de parámetros.
5. En Copy options (Opciones de copia), introduzca un nombre y una descripción para el nuevo grupo de parámetros de clúster. A continuación, elija Copy (Copiar) para guardar los cambios.

Using the AWS CLI

Para realizar una copia de un grupo de parámetros de clúster, utilice la operación `copy-db-cluster-parameter-group` con los siguientes parámetros.

- **`--source-db-cluster-parameter-group-identifier`**: obligatorio. El nombre o nombre de recurso de Amazon (ARN) del grupo de parámetros de clúster del que desea realizar una copia.

  Si los grupos de parámetros del clúster de origen y destino están en el mismo lugar Región de AWS, el identificador puede ser un nombre o un ARN.

  Si los grupos de parámetros del clúster de origen y destino son diferentes Regiones de AWS, el identificador debe ser un ARN.
- **`--target-db-cluster-parameter-group-identifier`**: obligatorio. El nombre o ARN del grupo de parámetros de clúster que se va a copiar.

  Restricciones:
  - No puede ser nulo ni estar vacío o en blanco.
  - Debe contener de 1 a 255 letras, números o guiones.

  - El primer carácter debe ser una letra.
  - No puede terminar con un guion ni contener dos guiones consecutivos.
- **`--target-db-cluster-parameter-group-description`**: obligatorio. Una descripción del usuario de la copia del grupo de parámetros de clúster.

Example

El siguiente código realiza una copia de `sample-parameter-group` y le asigna el nombre `sample-parameter-group-copy`.

Para Linux, macOS o Unix:

```
aws docdb copy-db-cluster-parameter-group \
    --source-db-cluster-parameter-group-identifier sample-parameter-group \
    --target-db-cluster-parameter-group-identifier sample-parameter-group-copy \
    --target-db-cluster-parameter-group-description "Copy of sample-parameter-group"
```

Para Windows:

```
aws docdb copy-db-cluster-parameter-group ^
    --source-db-cluster-parameter-group-identifier sample-parameter-group ^
    --target-db-cluster-parameter-group-identifier sample-parameter-group-copy ^
    --target-db-cluster-parameter-group-description "Copy of sample-parameter-group"
```

La salida de esta operación será similar a lo que se indica a continuación (formato JSON).

```
{
    "DBClusterParameterGroup": {
        "DBClusterParameterGroupArn": "arn:aws:rds:us-east-1:123456789012:cluster-
pg:sample-parameter-group-copy",
        "DBClusterParameterGroupName": "sample-parameter-group-copy",
        "DBParameterGroupFamily": "docdb4.0",
        "Description": "Copy of sample-parameter-group"
    }
}
```

Restablecimiento de grupos de parámetros de clúster de Amazon DocumentDB

Puede restablecer algunos o todos los valores de parámetros de un grupo de parámetros de clúster de Amazon DocumentDB a sus valores predeterminados utilizando Consola de administración de AWS o AWS Command Line Interface (AWS CLI) para restablecer el grupo de parámetros del clúster.

Using the Consola de administración de AWS

Siga estos pasos para restablecer algunos o todos los valores de parámetros de un grupo de parámetros de clúster a sus valores predeterminados.

Restablecimiento de los valores de parámetros de un grupo de parámetros de clúster

1. Inicie sesión en y abra la Consola de administración de AWS consola de Amazon DocumentDB en https://console.aws.amazon.com /docdb.
2. En el panel de navegación del lado izquierdo de la consola, elija Parameter groups (Grupos de parámetros).
3. En el panel Cluster parameter groups (Grupos de parámetros del clúster), seleccione el nombre del grupo de parámetros de clúster que quiera reiniciar.
4. Elija Actions (Acciones), y, a continuación, elija Reset (Reiniciar) para restablecer ese grupo de parámetros.
5. En la página de confirmación de restablecimiento del grupo de parámetros del clúster resultante, confirme que desea restablecer todos los parámetros del clúster de ese grupo de parámetros a sus valores predeterminados. A continuación, seleccione Reset (Restablecer) para restablecer el grupo de parámetros. También puede seleccionar Cancel (Cancelar) para descartar los cambios.

Using the AWS CLI

Para restablecer algunos o todos los valores de parámetros de un grupo de parámetros de clúster a sus valores predeterminados, use la operación `reset-db-cluster-parameter-group` con los siguientes parámetros.

- **`--db-cluster-parameter-group-name`**: obligatorio. El nombre del grupo de parámetros de clúster que se va a restablecer.

- **`--parameters`**: opcional. Una lista de `ParameterName` y `ApplyMethod` del grupo de parámetros de clúster que se va a restablecer a sus valores predeterminados. Los parámetros estáticos se deben establecer en `pending-reboot` para que se apliquen la próxima vez que se reinicie la instancia o en la siguiente solicitud `reboot-db-instance`. Debe llamar a `reboot-db-instance` para cada instancia del clúster a la que desee aplicar el parámetro estático actualizado.

  Este parámetro y `--reset-all-parameters` se excluyen mutuamente: puede utilizar uno pero no ambos.

- **`--reset-all-parameters`** o **`--no-reset-all-parameters`**: opcional. Especifica si se deben restablecer todos los parámetros (`--reset-all-parameters`) o solo algunos de los parámetros (`--no-reset-all-parameters`) a sus valores predeterminados. El parámetro `--reset-all-parameters` y `--parameters` se excluyen mutuamente: puede utilizar uno pero no ambos.

  Cuando restablece todo el grupo, los parámetros dinámicos se actualizan inmediatamente. Los parámetros estáticos se establecen en `pending-reboot` para que se apliquen la próxima vez que se reinicie la instancia o en la siguiente solicitud `reboot-db-instance`. Debe llamar a `reboot-db-instance` para cada instancia del clúster a la que desee aplicar el parámetro estático actualizado.

Example

Ejemplo 1: restablecimiento de todos los parámetros a sus valores predeterminados

El siguiente código restablece todos los parámetros del grupo de parámetros de clúster `sample-parameter-group` a sus valores predeterminados.

Para Linux, macOS o Unix:

```
aws docdb reset-db-cluster-parameter-group \
       --db-cluster-parameter-group-name sample-parameter-group \
       --reset-all-parameters
```

Para Windows:

```
aws docdb reset-db-cluster-parameter-group ^
       --db-cluster-parameter-group-name sample-parameter-group ^
```

```
       --reset-all-parameters
```

Ejemplo 2: restablecimiento de los parámetros especificados a sus valores predeterminados

El siguiente código restablece el parámetro `tls` del grupo de parámetros de clúster `sample-parameter-group` a su valor predeterminado.

Para Linux, macOS o Unix:

```
aws docdb reset-db-cluster-parameter-group \
       --db-cluster-parameter-group-name sample-parameter-group \
       --no-reset-all-parameters \
       --parameters ParameterName=tls,ApplyMethod=pending-reboot
```

Para Windows:

```
aws docdb reset-db-cluster-parameter-group ^
       --db-cluster-parameter-group-name sample-parameter-group ^
       --no-reset-all-parameters ^
       --parameters ParameterName=tls,ApplyMethod=pending-reboot
```

La salida de esta operación será similar a lo que se indica a continuación (formato JSON).

```
{
       "DBClusterParameterGroupName": "sample-parameter-group"
   }
```

Reinicio de una instancia del clúster

Antes de que el valor de un parámetro estático cambie, la instancia del clúster debe reiniciarse. Reinicie cada instancia del clúster a la que desee aplicar el parámetro estático actualizado.

Para Linux, macOS o Unix:

```
aws docdb reboot-db-instance \
       --db-instance-identifier sample-cluster-instance
```

Para Windows:

```
aws docdb reboot-db-instance ^
       --db-instance-identifier sample-cluster-instance
```

Borrado de grupos de parámetros de clúster de Amazon DocumentDB

Puede eliminar un grupo de parámetros de clúster de Amazon DocumentDB personalizado mediante Consola de administración de AWS o AWS Command Line Interface ()AWS CLI. No se puede eliminar el grupo de parámetros del clúster `default.docdb4.0`.

Using the Consola de administración de AWS

Eliminación de un grupo de parámetros de clúster

1. Inicie sesión en y abra la Consola de administración de AWS consola de Amazon DocumentDB en https://console.aws.amazon.com /docdb.
2. En el panel de navegación, seleccione Grupos de parámetros.

   > **Tip**
   >
   > Si no ve el panel de navegación del lado izquierdo de la pantalla, seleccione el icono de menú
   > (≡)
   > en la esquina superior izquierda de la página.

3. En el panel Parameter groups (Grupos de parámetros), seleccione el botón de opción situado a la izquierda del grupo de parámetros de clúster que desea eliminar.
4. Elija Acciones y, a continuación, elija Eliminar.
5. En el panel de confirmación Delete (Eliminar) elija Delete (Eliminar) para eliminar el grupo de parámetros del clúster. Para mantener el grupo de parámetros del clúster, elija Cancel (Cancelar).

Using the AWS CLI

Para eliminar un grupo de parámetros de clúster, utilice la operación `delete-db-cluster-parameter-group` con el siguiente parámetro.

- **`--db-cluster-parameter-group-name`**: obligatorio. El nombre del grupo de parámetros de clúster que se va a eliminar. Debe ser un grupo de parámetros de clúster existente. No se puede eliminar el grupo de parámetros del clúster *`default.docdb4.0`*.

Example - Eliminación de un grupo de parámetros de clúster

En el siguiente ejemplo, se presentan los tres pasos para eliminar un grupo de parámetros de clúster:

1. Buscar el nombre del grupo de parámetros de clúster que desea eliminar.
2. Eliminar el grupo de parámetros de clúster especificado.
3. Verificar que el grupo de parámetros de clúster se ha eliminado.

1. Busque el nombre del grupo de parámetros de clúster que desea eliminar.

El siguiente código muestra los nombres de todos los grupos de parámetros de clúster.

Para Linux, macOS o Unix:

```
aws docdb describe-db-cluster-parameter-groups \
       --query 'DBClusterParameterGroups[*].[DBClusterParameterGroupName]'
```

Para Windows:

```
aws docdb describe-db-cluster-parameter-groups ^
       --query 'DBClusterParameterGroups[*].[DBClusterParameterGroupName]'
```

El resultado de la operación anterior es una lista de los nombres de grupos de parámetros de clúster similar a la siguiente (formato JSON).

```
[
       [
           "default.docdb4.0"
       ],
       [
           "sample-parameter-group"
       ],
       [
           "sample-parameter-group-copy"
       ]
   ]
```

2. Elimine un grupo de parámetros de clúster.

El siguiente código elimina el grupo de parámetros de clúster `sample-parameter-group-copy`.

Para Linux, macOS o Unix:

```
aws docdb delete-db-cluster-parameter-group \
       --db-cluster-parameter-group-name sample-parameter-group-copy
```

Para Windows:

```
aws docdb delete-db-cluster-parameter-group ^
       --db-cluster-parameter-group-name sample-parameter-group-copy
```

Esta operación no muestra ningún resultado.

3. Verifique que el grupo de parámetros de clúster especificado se ha eliminado.

El siguiente código muestra los nombres de todos los grupos de parámetros de clúster restantes.

Para Linux, macOS o Unix:

```
aws docdb describe-db-cluster-parameter-groups \
       --query 'DBClusterParameterGroups[*].[DBClusterParameterGroupName]'
```

Para Windows:

```
aws docdb describe-db-cluster-parameter-groups ^
       --query 'DBClusterParameterGroups[*].[DBClusterParameterGroupName]'
```

El resultado de la operación anterior es una lista de los grupos de parámetros de clúster similar a la siguiente (formato JSON). El grupo de parámetros de clúster que acaba de eliminar no debe estar en la lista.

La salida de esta operación será similar a lo que se indica a continuación (formato JSON).

```
[
       [
           "default.docdb4.0"
       ],
       [
           "sample-parameter-group"
       ]
```

```
]
```

Referencia de parámetros de clúster de Amazon DocumentDB

Cuando se modifica un parámetro dinámico y se guarda el grupo de parámetros de clúster, el cambio se aplica inmediatamente, sea cual sea el estado de Apply Immediately (Aplicar inmediatamente). Cuando se cambia un parámetro estático y se guarda el grupo de parámetros de clúster, el cambio de parámetros tiene efecto después de reiniciar manualmente la instancia. Puede reiniciar una instancia mediante la consola de Amazon DocumentDB o llamar de forma explícita a `reboot-db-instance`.

En la tabla siguiente, se muestran todos los parámetros que se aplican a todas las instancias de un clúster de Amazon DocumentDB.

Parámetros a nivel de clúster de Amazon DocumentDB

Parámetro	Predeterminado	Valores válidos	Modificable	Tipo de aplicación	Tipo de datos	Description (Descripción)
`audit_logs`	disabled	activado, desactivado, ddl, dml_read, dml_write, todos, ninguno	Sí	Dinámico	Cadena	Define si los registros CloudWatch de auditoría de Amazon están habilitados. • **`enabled`**—los registros de CloudWatch auditoría están

Parámetro	Predeterminado	Valores válidos	Modificable	Tipo de aplicación	Tipo de datos	Description (Descripción)
						habilitados. • **`disabled`**—los registros de CloudWatch auditoría están deshabilitados. • **`ddl`**: la auditoría de eventos de DDL está habilitada. • **`dml_read`**: la auditoría de eventos de escritura de DML está habilitada.

Parámetro	Predeterminado	Valores válidos	Modificable	Tipo de aplicación	Tipo de datos	Description (Descripción)
						• **`dml_write`**: la auditoría de eventos de escritura de DML está habilitada. • **`all`**: la auditoría de todos los eventos de la base de datos está habilitada. • **`none`**: la auditoría está deshabilitada.

Parámetro	Predeterminado	Valores válidos	Modificable	Tipo de aplicación	Tipo de datos	Description (Descripción)
`change_stream_log_retention_duration`	10800	3600-604800	Sí	Dinámico	Entero	Define la duración (en segundos) que se conserva y se puede consumir el registro del flujo de cambios.

Parámetro	Predeterminado	Valores válidos	Modificable	Tipo de aplicación	Tipo de datos	Description (Descripción)
`default_collection_compression`	disabled	activado, desactivado (Amazon DocumentDB 5.0)/ zstd, lz4, ninguno (Amazon Document .0) DB8	Sí	Dinámico	Cadena	Define la configuración de compresión predeterminada para las nuevas colecciones de un clúster • **`enabled`**—La compresión Lz4 está habilitada de forma predeterminada en Amazon DocumentDB 5.0. La compresión zstd está habilitada de forma predeterminada en

Parámetro	Predeterminado	Valores válidos	Modificable	Tipo de aplicación	Tipo de datos	Description (Descripción)
						Amazon DocumentDB 8.0. • **`disabled, none`**— la compresión está deshabilitada de forma predeterminada (deshabilitada en Amazon DocumentDB 5.0, ninguna en Amazon DocumentDB 8.0).

Parámetro	Predeterminado	Valores válidos	Modificable	Tipo de aplicación	Tipo de datos	Description (Descripción)
`profiler`	disabled	habilitado, deshabilitado	Sí	Dinámico	Cadena	Habilita la creación de perfiles para operaciones lentas. • **`enabled`**— las operaciones que tardan más que un valor límite definido por el cliente (por ejemplo, 100 ms) se registran en Amazon Logs. CloudWatch • **`disabled`**— las operaciones lentas no se

Parámetro	Predeterminado	Valores válidos	Modificable	Tipo de aplicación	Tipo de datos	Description (Descripción)
						registran en Logs. CloudWatch
`profiler_sampling_rate`	1.0	0,0-1,0	Sí	Dinámico	Flotante	Define la velocidad de muestreo para las operaciones registradas.

Parámetro	Predeterminado	Valores válidos	Modificable	Tipo de aplicación	Tipo de datos	Description (Descripción)
`profiler_threshold_ms`	100	50-2147483646	Sí	Dinámico	Entero	Define el umbral de `profiler`. • Todas las operaciones superiores a `profiler_threshold_ms` las se registran en los CloudWatch registros.

Parámetro	Predeterminado	Valores válidos	Modificable	Tipo de aplicación	Tipo de datos	Description (Descripción)
`planner_version`	3.0	1,0, 2,0, 3,0	Sí	Dinámico	Flotante	Define la versión del planificador de consultas que se utilizará en las consultas. • **`1.0`**— Compatible con Amazon DocumentDB 5.0. • **`2.0`**— Mejoras en la búsqueda y actualización de los operadores. Compatible con Amazon DocumentDB 5.0.

Parámetro	Predeterminado	Valores válidos	Modificable	Tipo de aplicación	Tipo de datos	Description (Descripción)
						• **`3.0`**— Mejoras en la búsqueda, actualización y agregación de operadores. Planificador de consultas predeterminado en Amazon DocumentDB 8.0.

Parámetro	Predeterminado	Valores válidos	Modificable	Tipo de aplicación	Tipo de datos	Description (Descripción)
`tls`	enabled	habilitado, deshabilitado, fips-140-3, tls1.2+, tls1.3+	Sí	Estático	Cadena	Define si son obligatorias las conexiones TLS (Transport Layer Security). • **`enabled`**: se requieren conexiones TLS para conectarse. • **`disabled`**: las conexiones TLS no se pueden usar para conectarse. • **`fips-140-3`** : para conectarse, se

Parámetro	Predeterminado	Valores válidos	Modificable	Tipo de aplicación	Tipo de datos	Description (Descripción)
						requieren conexiones TLS con atributos de Federal Information Processing Standards Publications (FIPS, Publicaciones de los Estándares de procesamiento de la información federal). El clúster solo acepta conexiones seguras según la

Parámetro	Predeterminado	Valores válidos	Modificable	Tipo de aplicación	Tipo de datos	Description (Descripción)
						publicación 140-3 de las FIPS. Esto solo se admite a partir de los clústeres de Amazon DocumentDB 5.0 (versión del motor 3.0.3727) en estas regiones: ca-central-1, us-west-2, us-east-1, us-east-2, -1, -1. us-gov-east us-gov-west

Parámetro	Predeterminado	Valores válidos	Modificable	Tipo de aplicación	Tipo de datos	Description (Descripción)
						• **`tls1.2+`**: se requieren conexiones TLS que utilicen la versión 1.2 o superior de TLS para conectarse. Esto solo se admite a partir de Amazon DocumentDB 4.0 (versión de motor 2.0.10980) y Amazon DocumentDB 5.0 (versión de motor 3.0.11051).

Parámetro	Predeterminado	Valores válidos	Modificable	Tipo de aplicación	Tipo de datos	Description (Descripción)
						• **`tls1.3+`**: se requieren conexiones TLS que utilicen la versión 1.3 o superior de TLS para conectarse. Esto solo se admite a partir de Amazon DocumentDB 4.0 (versión de motor 2.0.10980) y Amazon DocumentDB 5.0 (versión de motor 3.0.11051).

Parámetro	Predeterminado	Valores válidos	Modificable	Tipo de aplicación	Tipo de datos	Description (Descripción)
`ttl_monitor`	enabled	habilitado, deshabilitado	Sí	Dinámico	Cadena	Define si la monitorización de tiempo de vida (TTL) está habilitada para el clúster. • **`enabled`**: la supervisión de TTL está habilitada. • **`disabled`**: la supervisión de TTL está deshabilitada.

Modificación de parámetros de clúster de Amazon DocumentDB

En Amazon DocumentDB, los grupos de parámetros de clúster constan de parámetros que se aplican a todas las instancias que cree en el clúster. En los grupos de parámetros de clúster personalizados, puede modificar un valor de parámetro en cualquier momento o restablecer todos los valores de parámetro a sus valores predeterminados para los grupos de parámetros que cree. En

esta sección se describe cómo ver los parámetros que conforman un grupo de parámetros de clúster de Amazon DocumentDB y sus valores, y cómo cambiar o actualizar estos valores.

Los parámetros pueden ser dinámicos o estáticos. Cuando se modifica un parámetro dinámico y se guarda el grupo de parámetros de clúster, el cambio se aplica inmediatamente, sea cual sea el estado de `Apply Immediately`. Cuando se cambia un parámetro estático y se guarda el grupo de parámetros de clúster, el cambio de parámetros solo tiene efecto después de reiniciar manualmente la instancia.

Visualización de los parámetros de un grupo de parámetros de clúster de Amazon DocumentDB

Para ver los parámetros y valores de un clúster de Amazon DocumentDB, utilice o. Consola de administración de AWS AWS CLI

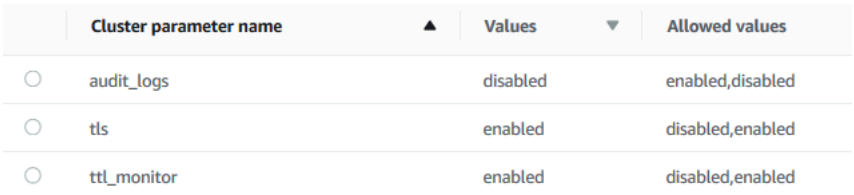
Using the Consola de administración de AWS

Visualización de los detalles de un grupo de parámetros de clúster

1. Inicie sesión en y abra la Consola de administración de AWS consola de Amazon DocumentDB en https://console.aws.amazon.com /docdb.
2. En el panel de navegación, seleccione Grupos de parámetros.

   > **Tip**
   >
   > Si no ve el panel de navegación del lado izquierdo de la pantalla, seleccione el icono de menú
   > (≡)
   > en la esquina superior izquierda de la página.

3. En el panel Parameter groups (Grupos de parámetros), seleccione el nombre del grupo de parámetros de clúster cuyos detalles desee ver.
4. La página resultante muestra los siguientes valores para cada parámetro: el nombre del parámetro, el valor actual, los valores permitidos, si el parámetro es modificable, el tipo de aplicación, el tipo de datos y la descripción.



Using the AWS CLI

Para ver los parámetros de un grupo de parámetros de un clúster y sus valores, utilice la operación `describe-db-cluster-parameters` con los siguientes parámetros.

- **`--db-cluster-parameter-group-name`**: obligatorio. El nombre del grupo de parámetros de clúster para el que desea obtener una lista detallada de parámetros.
- **`--source`**: opcional. Si se especifica, devuelve solo los parámetros de un origen específico. Los orígenes de parámetros pueden ser `engine-default`, `system` o `user`.

Example

El siguiente código de ejemplo muestra los parámetros, junto con sus valores, del grupo de parámetros `custom3-6-param-grp`. Para obtener más información sobre el grupo de parámetros, omita la línea `--query`. Para obtener más información sobre todos los grupos de parámetros, omita la línea `--db-cluster-parameter-group-name`.

Para Linux, macOS o Unix:

```
aws docdb describe-db-cluster-parameters \
   --db-cluster-parameter-group-name custom3-6-param-grp \
   --query 'Parameters[*].[ParameterName,ParameterValue]'
```

Para Windows:

```
aws docdb describe-db-cluster-parameters ^
   --db-cluster-parameter-group-name custom3-6-param-grp ^
   --query 'Parameters[*].[ParameterName,ParameterValue]'
```

La salida de esta operación será similar a lo que se indica a continuación (formato JSON).

```
[
    [
        "audit_logs",
        "disabled"
    ],
    [
        "tls",
        "enabled"
```

```
    ],
    [
        "ttl_monitor",
        "enabled"
    ]
]
```

Modificación de los parámetros de un grupo de parámetros de clúster de Amazon DocumentDB

Puede modificar los parámetros de un grupo de parámetros con las teclas o. Consola de administración de AWS AWS CLI

Using the Consola de administración de AWS

Actualización de los parámetros de un grupo de parámetros de clúster

1. Inicie sesión en y abra la Consola de administración de AWS consola de Amazon DocumentDB en https://console.aws.amazon.com /docdb.
2. En el panel de navegación, seleccione Grupos de parámetros.

> **Tip**
>
> Si no ve el panel de navegación del lado izquierdo de la pantalla, seleccione el icono de menú
> (≡)
> en la esquina superior izquierda de la página.

3. En el panel Parameter groups (Grupos de parámetros), elija el grupo de parámetros del clúster cuyos parámetros desea actualizar.
4. La página resultante muestra los parámetros y sus detalles correspondientes para este grupo de parámetros de clúster. Seleccione un parámetro para actualizar.
5. En la parte superior derecha de la página, elija Edit (Editar) para cambiar el valor del parámetro. Para obtener más información sobre los tipos de parámetros de clúster, consulte Referencia de parámetros de clúster de Amazon DocumentDB.
6. Realice el cambio y, a continuación, elija Modify cluster parameter (Modificar parámetro de clúster) para guardar los cambios. Para descartar los cambios, selecciona Cancel (Cancelar).

Using the AWS CLI

Para modificar los parámetros de un grupo de parámetros de clúster, utilice la operación `modify-db-cluster-parameter-group` con los siguientes parámetros.

- **`--db-cluster-parameter-group-name`**: obligatorio. El nombre del grupo de parámetros de clúster que va a modificar.
- **`--parameters`**: obligatorio. El parámetro o los parámetros que va a modificar. Cada entrada de parámetro debe incluir lo siguiente:
  - **`ParameterName`**: el nombre del grupo de parámetros de clúster que va a modificar.
  - **`ParameterValue`**: el valor nuevo de este parámetro de clúster.
  - **`ApplyMethod`**: cómo desea que se apliquen los cambios a este parámetro. Los valores permitidos son `immediate` y `pending-reboot`.

> **Note**
>
> Los parámetros con el `ApplyType` de `static` deben tener un `ApplyMethod` de `pending-reboot`.

Para cambiar los valores de los parámetros de un grupo de parámetros de clúster (AWS CLI)

En el siguiente ejemplo se cambia el nombre del parámetro `tls`.

1. Muestre los parámetros y sus valores de **`sample-parameter-group`**

   Para Linux, macOS o Unix:

   ```
   aws docdb describe-db-cluster-parameters \
       --db-cluster-parameter-group-name sample-parameter-group
   ```

   Para Windows:

   ```
   aws docdb describe-db-cluster-parameters ^
       --db-cluster-parameter-group-name sample-parameter-group
   ```

   La salida de esta operación será similar a lo que se indica a continuación (formato JSON).

```
{
    "Parameters": [
        {
            "Source": "system",
            "ApplyType": "static",
            "AllowedValues": "disabled,enabled",
            "ParameterValue": "enabled",
            "ApplyMethod": "pending-reboot",
            "DataType": "string",
            "ParameterName": "tls",
            "IsModifiable": true,
            "Description": "Config to enable/disable TLS"
        },
        {
            "Source": "user",
            "ApplyType": "dynamic",
            "AllowedValues": "disabled,enabled",
            "ParameterValue": "enabled",
            "ApplyMethod": "pending-reboot",
            "DataType": "string",
            "ParameterName": "ttl_monitor",
            "IsModifiable": true,
            "Description": "Enables TTL Monitoring"
        }
    ]
}
```

2. Modifique el parámetro **`tls`** para que su valor sea **`disabled`**. No se puede modificar `ApplyMethod` ya que `ApplyType` es `static`.

   Para Linux, macOS o Unix:

```
aws docdb modify-db-cluster-parameter-group \
    --db-cluster-parameter-group-name sample-parameter-group \
    --parameters
 "ParameterName"=tls,ParameterValue=disabled,ApplyMethod=pending-reboot"
```

   Para Windows:

```
aws docdb modify-db-cluster-parameter-group ^
    --db-cluster-parameter-group-name sample-parameter-group ^
```

```
    --parameters "ParameterName=tls,ParameterValue=disabled,ApplyMethod=pending-
reboot"
```

La salida de esta operación será similar a lo que se indica a continuación (formato JSON).

```
{
    "DBClusterParameterGroupName": "sample-parameter-group"
}
```

3. Espere al menos 5 minutos.
4. Muestre los valores de parámetro de **`sample-parameter-group`**.

   Para Linux, macOS o Unix:

```
aws docdb describe-db-cluster-parameters \
    --db-cluster-parameter-group-name sample-parameter-group
```

   Para Windows:

```
aws docdb describe-db-cluster-parameters ^
    --db-cluster-parameter-group-name sample-parameter-group
```

   La salida de esta operación será similar a lo que se indica a continuación (formato JSON).

```
{
    "Parameters": [
        {
            "ParameterName": "audit_logs",
            "ParameterValue": "disabled",
            "Description": "Enables auditing on cluster.",
            "Source": "system",
            "ApplyType": "dynamic",
            "DataType": "string",
            "AllowedValues": "enabled,disabled",
            "IsModifiable": true,
            "ApplyMethod": "pending-reboot"
        },
        {
            "ParameterName": "tls",
            "ParameterValue": "disabled",
            "Description": "Config to enable/disable TLS",
```

```
            "Source": "user",
            "ApplyType": "static",
            "DataType": "string",
            "AllowedValues": "disabled,enabled",
            "IsModifiable": true,
            "ApplyMethod": "pending-reboot"
        }
    ]
}
```

Descripción de los puntos de conexión de Amazon DocumentDB

Puede usar los puntos de conexión de Amazon DocumentDB (con compatibilidad con MongoDB) para conectarse a un clúster o a una instancia. Amazon DocumentDB tiene tres tipos diferentes de puntos de conexión, cada uno con su propia finalidad.

Temas

- Búsqueda de puntos de conexión de un clúster
- Búsqueda del punto de conexión de una instancia
- Conexión a puntos de conexión

Punto de conexión de clúster

Un punto de conexión de clúster es un punto de conexión de un clúster de Amazon DocumentDB que se conecta a la instancia principal actual del clúster. Cada clúster de Amazon DocumentDB tiene un solo punto de conexión de clúster y una sola instancia principal. En caso de que se produzca una conmutación por error, el punto de conexión del clúster se reasigna a la nueva instancia principal.

Punto de conexión del lector

Un punto de conexión del lector es un punto de conexión de un clúster de Amazon DocumentDB que se conecta a una de las réplicas disponibles de ese clúster. Cada clúster de base de datos de Amazon DocumentDB tiene un punto de conexión del lector. Si hay más de una réplica, el punto de conexión del lector dirige cada solicitud de conexión a una de las réplicas de Amazon DocumentDB.

Punto de conexión de instancia

Un punto de conexión de una instancia es aquel que se conecta a una instancia específica. Cada instancia de un clúster, independientemente de si es una instancia principal o de réplica, tiene su propio punto de conexión de instancia único. Es mejor no usar puntos de conexión de instancias en las aplicaciones. Esto se debe a que pueden cambiar los roles en caso de una conmutación por error, lo que obligaría a realizar modificaciones en el código de la aplicación.

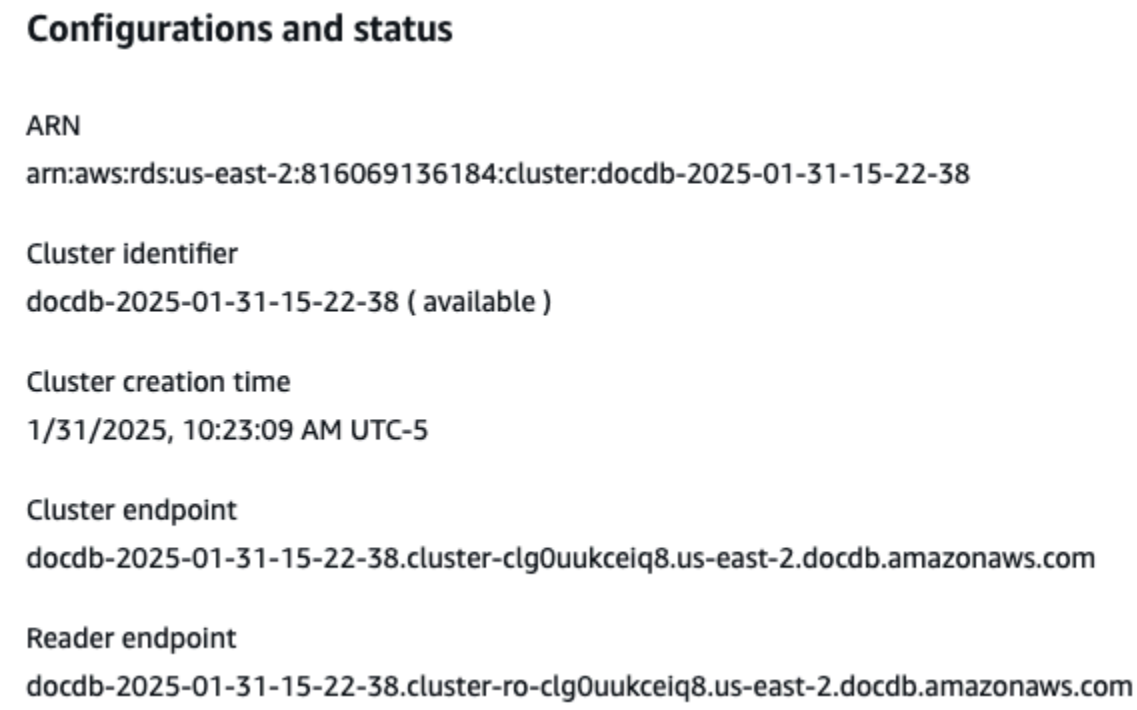
Búsqueda de puntos de conexión de un clúster

Puede buscar el punto de conexión de clúster de un clúster y el punto de conexión del lector mediante la consola de Amazon DocumentDB o la AWS CLI.

Using the Consola de administración de AWS

Cómo encontrar los puntos de conexión de un clúster mediante la consola:

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon DocumentDB en https://console.aws.amazon.com/docdb.
2. En el panel de navegación, seleccione Clusters (Clústeres).
3. En la lista de clústeres, seleccione el nombre del clúster de su interés.
4. En la página de detalles del clúster, elija la pestaña Configuración. En la sección Configuraciones y estado, encontrará el Punto de conexión del clúster y el Punto de conexión del lector.



5. Para conectarse a este clúster, seleccione la pestaña Conectividad y seguridad. Localice la cadena de conexión del shell de `mongo` y una cadena de conexión que pueda utilizar en el código de la aplicación para conectarse a su clúster.



Using the AWS CLI

Para buscar los puntos de conexión del clúster y del lector para su clúster con la AWS CLI, ejecute el comando `describe-db-clusters` con estos parámetros.

Parámetros

- **`--db-cluster-identifier`**: opcional. Especifica el clúster para el que se van a devolver puntos de conexión. Si se omite, devuelve los puntos de conexión de hasta 100 clústeres.

- **`--query`**: opcional. Especifica los campos para mostrar. Sirve para reducir la cantidad de datos que se necesitan consultar para encontrar los puntos de conexión. Si se omite, se devuelve toda la información de un clúster.
- **`--region`**: opcional. Utilice el parámetro `--region` para especificar la región a la que desea aplicar el comando. Si se omite, se utiliza la región predeterminada.

Example

En el siguiente ejemplo, se devuelve el punto de conexión `DBClusterIdentifier` (punto de conexión del clúster) y `ReaderEndpoint` para `sample-cluster`.

Para Linux, macOS o Unix:

```
aws docdb describe-db-clusters \
   --region us-east-1 \
   --db-cluster-identifier sample-cluster \
   --query 'DBClusters[*].[DBClusterIdentifier,Port,Endpoint,ReaderEndpoint]'
```

Para Windows:

```
aws docdb describe-db-clusters ^
   --region us-east-1 ^
   --db-cluster-identifier sample-cluster ^
   --query 'DBClusters[*].[DBClusterIdentifier,Port,Endpoint,ReaderEndpoint]'
```

La salida de esta operación será similar a lo que se indica a continuación (formato JSON).

```
[
  [
     "sample-cluster",
     27017,
     "sample-cluster.cluster-corlsfccjozr.us-east-1.docdb.amazonaws.com",
     "sample-cluster.cluster-ro-corlsfccjozr.us-east-1.docdb.amazonaws.com"
  ]
]
```

Ahora que tiene el punto de conexión del clúster, puede conectarse al clúster mediante `mongo` o `mongodb`. Para obtener más información, consulte Conexión a puntos de conexión.

Búsqueda del punto de conexión de una instancia

Puede encontrar los puntos de conexión para una instancia de base de datos mediante la consola de Amazon DocumentDB o la AWS CLI.

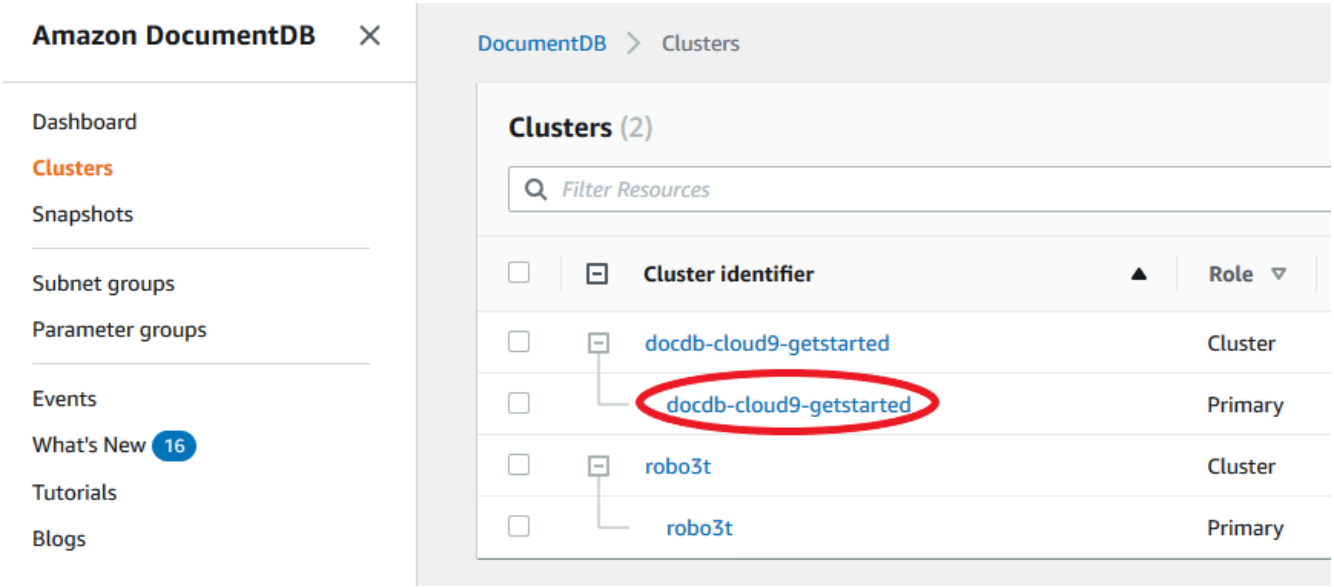
Using the Consola de administración de AWS

Búsqueda del punto de conexión de una instancia mediante la consola

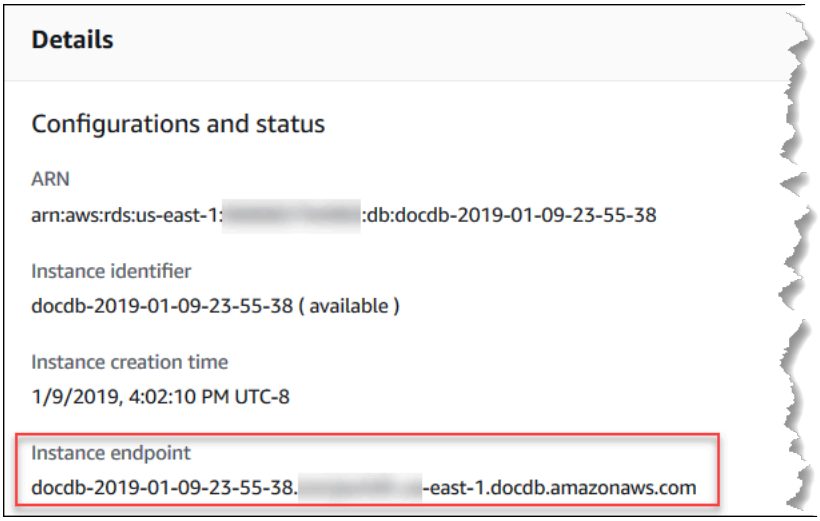
1. Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon DocumentDB en https://console.aws.amazon.com/docdb.
2. En el panel de navegación, seleccione Clusters (Clústeres).

> **Tip**
>
> Si no ve el panel de navegación del lado izquierdo de la pantalla, seleccione el icono de menú
> (≡)
> en la esquina superior izquierda de la página.

3. En el cuadro de navegación de clústeres, verá la columna Identificador del clúster. Las instancias se muestran en clústeres, de forma similar a la siguiente captura de pantalla.



4. Marque la casilla de verificación situada a la izquierda de la instancia de su interés.
5. Desplácese hacia abajo hasta la sección Details (Detalles) y localice el punto de conexión de la instancia.



6. Para conectarse a esta instancia, desplácese hacia abajo hasta la sección Connect (Conexión). Localice la cadena de conexión del shell de `mongo` y una cadena de conexión que pueda utilizar en el código de su aplicación para conectarse a su instancia.



Using the AWS CLI

Para buscar el punto de conexión de la instancia mediante la AWS CLI, ejecute el siguiente comando con estos argumentos.

Argumentos

- **`--db-instance-identifier`**: opcional. Especifica la instancia para la que se va a devolver el punto de conexión. Si se omite, se devuelve el punto de conexión de hasta 100 instancias.
- **`--query`**: opcional. Especifica los campos para mostrar. Sirve para reducir la cantidad de datos que se necesitan consultar para encontrar los puntos de conexión. Si se omite, se devuelve toda la información de la instancia. El campo `Endpoint` tiene tres miembros, por lo que la consulta del siguiente ejemplo devuelve los tres miembros. Si solo está interesado en algunos de los miembros de `Endpoint` sustituya `Endpoint` en la consulta por los miembros de su interés, tal y como se muestra en el segundo ejemplo.

- **`--region`**: opcional. Utilice el parámetro `--region` para especificar la región a la que desea aplicar el comando. Si se omite, se utiliza la región predeterminada.

Example

Para Linux, macOS o Unix:

```
aws docdb describe-db-instances \
    --region us-east-1 \
    --db-instance-identifier sample-cluster-instance \
    --query 'DBInstances[*].[DBInstanceIdentifier,Endpoint]'
```

Para Windows:

```
aws docdb describe-db-instances ^
    --region us-east-1 ^
    --db-instance-identifier sample-cluster-instance ^
    --query 'DBInstances[*].[DBInstanceIdentifier,Endpoint]'
```

La salida de esta operación será similar a lo que se indica a continuación (formato JSON).

```
[
    [
        "sample-cluster-instance",
        {
            "Port": 27017,
            "Address": "sample-cluster-instance.corcjozrlsfc.us-
east-1.docdb.amazonaws.com",
            "HostedZoneId": "Z2R2ITUGPM61AM"
        }
    ]
]
```

Reduciendo el resultado para eliminar el `HostedZoneId` del punto de conexión, puede modificar su consulta especificando `Endpoint.Port` y `Endpoint.Address`.

Para Linux, macOS o Unix:

```
aws docdb describe-db-instances \
    --region us-east-1 \
    --db-instance-identifier sample-cluster-instance \
```

```
    --query 'DBInstances[*].[DBInstanceIdentifier,Endpoint.Port,Endpoint.Address]'
```

Para Windows:

```
aws docdb describe-db-instances ^
    --region us-east-1 ^
    --db-instance-identifier sample-cluster-instance ^
    --query 'DBInstances[*].[DBInstanceIdentifier,Endpoint.Port,Endpoint.Address]'
```

La salida de esta operación será similar a lo que se indica a continuación (formato JSON).

```
[
    [
        "sample-cluster-instance",
        27017,
        "sample-cluster-instance.corcjozrlsfc.us-east-1.docdb.amazonaws.com"
    ]
]
```

Ahora que tiene el punto de conexión de la instancia, puede conectarse a la instancia mediante mongo o mongodb. Para obtener más información, consulte Conexión a puntos de conexión.

Conexión a puntos de conexión

Cuando tenga su punto de conexión, ya sea del clúster o de la instancia, puede conectarse a él utilizando el shell de mongo o una cadena de conexión.

Conexión mediante el shell de mongo

Utilice la siguiente estructura para crear la cadena que necesita para conectarse a su clúster o instancia mediante el shell de mongo:

```
mongo \
    --ssl \
    --host Endpoint:Port \
    --sslCAFile global-bundle.pem \
    --username UserName \
    --password Password
```

Ejemplos del shell de **mongo**

Conectarse a un clúster:

```
mongo \
    --ssl \
    --host sample-cluster.corcjozrlsfc.us-east-1.docdb.amazonaws.com:27017 \
    --sslCAFile global-bundle.pem \
    --username UserName \
    --password Password
```

Conectarse a una instancia:

```
mongo \
    --ssl \
    --host sample-cluster-instance.corcjozrlsfc.us-east-1.docdb.amazonaws.com:27017 \
    --sslCAFile global-bundle.pem \
    --username UserName \
    --password Password
```

Conexión mediante una cadena de conexión

Utilice la siguiente estructura para crear la cadena de conexión que necesita para conectarse a su clúster o instancia.

```
mongodb://UserName:Password@endpoint:port?replicaSet=rs0&ssl_ca_certs=global-
bundle.pem
```

Ejemplos de cadenas de conexión

Conectarse a un clúster:

```
mongodb://UserName:Password@sample-cluster.cluster-corlsfccjozr.us-
east-1.docdb.amazonaws.com:27017?replicaSet=rs0&ssl_ca_certs=global-bundle.pem
```

Conectarse a una instancia:

```
mongodb://UserName:Password@sample-cluster-instance.cluster-corlsfccjozr.us-
east-1.docdb.amazonaws.com:27017?replicaSet=rs0&ssl_ca_certs=global-bundle.pem
```

Descripción de los nombres de recursos de Amazon DocumentDB () ARNs

Cada uno de los recursos que cree AWS se identifica de forma única con un nombre de recurso de Amazon (ARN). Para determinadas operaciones de Amazon DocumentDB (compatible con MongoDB), debe identificar de forma inequívoca un recurso de Amazon DocumentDB mediante su ARN. Por ejemplo, cuando añade una etiqueta a un recurso, debe proporcionar el ARN del recurso.

Temas

- Creación de un ARN para un recurso de Amazon DocumentDB
- Búsqueda de un ARN de recurso de Amazon DocumentDB

Creación de un ARN para un recurso de Amazon DocumentDB

Puede crear un ARN para un recurso de Amazon DocumentDB utilizando la siguiente sintaxis. Amazon DocumentDB comparte el formato de Amazon Relational Database Service (Amazon RDS). ARNs Amazon DocumentDB ARNs contiene `rds` y no. `docdb`

`arn:aws:rds:`*`region`*`:`*`account_number`*`:`*`resource_type`*`:`*`resource_id`*

Nombre de la región	Region	Zonas de disponibilidad (cálculo)
Este de EE. UU. (Ohio)	`us-east-2`	3
Este de EE. UU. (Norte de Virginia)	`us-east-1`	6
Oeste de EE. UU. (Oregón)	`us-west-2`	4
África (Ciudad del Cabo)	`af-south-1`	3
América del Sur (São Paulo)	`sa-east-1`	3

Nombre de la región	Region	Zonas de disponibilidad (cálculo)
Asia-Pacífico (Hong Kong)	ap-east-1	3
Asia-Pacífico (Hyderabad)	ap-south-2	3
Asia-Pacífico (Malasia)	ap-southeast-5	3
Asia-Pacífico (Mumbai)	ap-south-1	3
Asia-Pacífico (Osaka)	ap-northeast-3	3
Asia-Pacífico (Seúl)	ap-northeast-2	4
Asia-Pacífico (Singapur)	ap-southeast-1	3
Asia-Pacífico (Sídney)	ap-southeast-2	3
Asia-Pacífico (Yakarta)	ap-southeast-3	3
Asia-Pacífico (Tailandia)	ap-southeast-7	3
Asia-Pacífico (Tokio)	ap-northeast-1	3
Canadá (centro)	ca-central-1	3
Región China (Pekín)	cn-north-1	3
China (Ningxia)	cn-northwest-1	3
Europa (Fráncfort)	eu-central-1	3
Europa (Irlanda)	eu-west-1	3

Nombre de la región	Region	Zonas de disponibilidad (cálculo)
Europa (Londres)	`eu-west-2`	3
Europa (Milán)	`eu-south-1`	3
Europa (París)	`eu-west-3`	3
Europa (España)	`eu-south-2`	3
Europa (Estocolmo)	`eu-north-1`	3
México (centro)	`mx-central-1`	3
Medio Oriente (EAU)	`me-central-1`	3
Israel (Tel Aviv)	`il-central-1`	3
AWS GovCloud (EE. UU.-Oeste)	`us-gov-west-1`	3
AWS GovCloud (Estados Unidos-Este)	`us-gov-east-1`	3

> **Note**
>
> La arquitectura de Amazon DocumentDB separa el almacenamiento y la computación. Para la capa de almacenamiento, Amazon DocumentDB replica seis copias de los datos en tres zonas de AWS disponibilidad (). AZs Las que AZs aparecen en la tabla anterior son las AZs que puede utilizar en una región determinada para aprovisionar instancias informáticas. Por ejemplo, si lanza un clúster de Amazon DocumentDB en ap-northeast-1, su almacenamiento se replicará de seis formas en tres, pero sus instancias de procesamiento solo estarán disponibles en dos. AZs AZs

En la siguiente tabla se muestra el formato que debe utilizar al crear un ARN para un tipo de recurso concreto de Amazon DocumentDB. Amazon DocumentDB comparte el formato de Amazon RDS. ARNs Amazon DocumentDB ARNs contiene `rds` y no. `docdb`

Tipo de recurso	Formato de ARN / Ejemplo
Instancia (db)	`arn:aws:rds:region:account_number:db:resource_id` `arn:aws:rds:us-east-1:1234567890:db:sample-db-instance`
Clúster (cluster)	`arn:aws:rds:region:account_number:cluster:resource_id` `arn:aws:rds:us-east-1:1234567890:cluster:sample-db-cluster`
Grupo de parámetros del clúster (cluster-pg)	`arn:aws:rds:region:account_number:cluster-pg:resource_id` `arn:aws:rds:us-east-1:1234567890:cluster-pg:sample-db-cluster-parameter-group`
Grupo de seguridad (secgrp)	`arn:aws:rds:region:account_number:secgrp:resource_id` `arn:aws:rds:us-east-1:1234567890:secgrp:sample-public-secgrp`
Instantánea de clúster (cluster-snapshot)	`arn:aws:rds:region:account_number:cluster-snapshot:resource_id` `arn:aws:rds:us-east-1:1234567890:cluster-snapshot:sample-db-cluster-snapshot`
Grupo de subredes (subgrp)	`arn:aws:rds:region:account_number:subgrp:resource_id`

Tipo de recurso	Formato de ARN / Ejemplo
	`arn:aws:rds:us-east-1:` *`1234567890`* `:subgrp:`*`sample-subnet-10`*

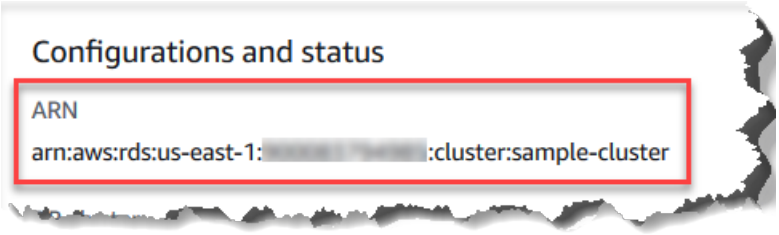
Búsqueda de un ARN de recurso de Amazon DocumentDB

Puede encontrar el ARN de un recurso de Amazon DocumentDB mediante Consola de administración de AWS el o el. AWS CLI

Using the Consola de administración de AWS

Para buscar un ARN mediante la consola, vaya al recurso cuyo ARN desea obtener y consulte los detalles de ese recurso.

Por ejemplo, puede obtener el ARN de un clúster desde la pestaña Configuración de los detalles del clúster. El ARN se encuentra en la sección Configuraciones y estado, como se muestra en la siguiente captura de pantalla.



Using the AWS CLI

Para obtener un ARN mediante un recurso concreto de Amazon DocumentDB, utilice `describe` la operación AWS CLI para ese recurso. En la tabla siguiente se muestran cada AWS CLI operación y la propiedad ARN que se utiliza con la operación para obtener un ARN.

AWS CLI Comando	Propiedad ARN
`describe-db-instances`	`DBInstanceArn`
`describe-db-clusters`	`DBClusterArn`
`describe-db-parameter-groups`	`DBParameterGroupArn`

AWS CLI Comando	Propiedad ARN
`describe-db-cluster-parameter-groups`	`DBClusterParameterGroupArn`
`describe-db-security-groups`	`DBSecurityGroupArn`
`describe-db-snapshots`	`DBSnapshotArn`
`describe-db-cluster-snapshots`	`DBClusterSnapshotArn`
`describe-db-subnet-groups`	`DBSubnetGroupArn`

Example - Búsqueda del ARN de un clúster

La siguiente AWS CLI operación busca el ARN del clúster. `sample-cluster`

Para Linux, macOS o Unix:

```
aws docdb describe-db-clusters \
    --db-cluster-identifier sample-cluster \
    --query 'DBClusters[*].DBClusterArn'
```

Para Windows:

```
aws docdb describe-db-clusters ^
    --db-cluster-identifier sample-cluster \
    --query 'DBClusters[*].DBClusterArn'
```

La salida de esta operación será similar a lo que se indica a continuación (formato JSON).

```
[
    "arn:aws:rds:us-east-1:123456789012:cluster:sample-cluster"
]
```

Example - ARNs Búsqueda de varios grupos de parámetros

Para Linux, macOS o Unix:

```
aws docdb describe-db-cluster-parameter-groups \
```

```
   --query 'DBClusterParameterGroups[*].DBClusterParameterGroupArn'
```

Para Windows:

```
aws docdb describe-db-cluster-parameter-groups ^
   --query 'DBClusterParameterGroups[*].DBClusterParameterGroupArn'
```

La salida de esta operación será similar a lo que se indica a continuación (formato JSON).

```
[
    "arn:aws:rds:us-east-1:123456789012:cluster-pg:custom3-6-param-grp",
    "arn:aws:rds:us-east-1:123456789012:cluster-pg:default.aurora5.6",
    "arn:aws:rds:us-east-1:123456789012:cluster-pg:default.docdb3.6"
]
```

Etiquetado de recursos de Amazon DocumentDB

Puede utilizar etiquetas de Amazon DocumentDB (con compatibilidad con MongoDB) para agregar metadatos a los recursos de Amazon DocumentDB. Estas etiquetas se pueden utilizar junto con políticas de AWS Identity and Access Management (IAM) para administrar el acceso a los recursos de Amazon DocumentDB y para controlar qué acciones se pueden aplicar a los recursos. También puede utilizar etiquetas para hacer un seguimiento de los costos, agrupando los gastos correspondientes en recursos con etiquetas similares.

Puede etiquetar los siguientes recursos de Amazon DocumentDB:

- Clústeres
- instancias
- Instantáneas
- Instantáneas del clúster
- Grupos de parámetros
- Grupos de parámetros de clústeres
- Grupos de seguridad
- Grupos de subredes

Información general de las etiquetas de recursos de Amazon DocumentDB

Las etiquetas de Amazon DocumentDB son pares nombre-valor que el usuario define y asocia a un recurso de Amazon DocumentDB. El nombre es la clave. Si lo desea puede proporcionar un valor para la clave o no. También puede usar etiquetas para asignar información arbitraria a un recurso de Amazon DocumentDB. Puede usar claves de etiqueta, por ejemplo, para definir una categoría, y el valor de la etiqueta puede ser un elemento dentro de esa categoría. Por ejemplo, puede definir una clave de etiqueta `project` y un valor de etiqueta de `Salix` para indicar que el recurso de Amazon DocumentDB se asigna al proyecto Salix. Asimismo, puede utilizar etiquetas para designar recursos de Amazon DocumentDB para pruebas o para producción mediante una clave como `environment=test` o `environment=production`. Se recomienda utilizar un conjunto coherente de claves de etiqueta que facilite el seguimiento de los metadatos asociados a los recursos de Amazon DocumentDB.

Puede usar etiquetas para organizar la factura de AWS de modo que refleje su propia estructura de costos. Para ello, inscríbase para obtener una factura de Cuenta de AWS que incluya valores de clave de etiquetas. A continuación, para ver los costos de los recursos combinados, organice la información de facturación de acuerdo con los recursos con los mismos valores de clave de etiquetas. Por ejemplo, puede etiquetar varios recursos con un nombre de aplicación específico y luego organizar su información de facturación para ver los costos totales de la aplicación en distintos servicios. Para obtener más información, consulte Uso de etiquetas de asignación de costos en la AWSGuía del usuario de Administración de facturación y costos.

Cada recurso de Amazon DocumentDB tiene un conjunto de etiquetas que contiene todas las etiquetas asignadas a ese recurso. Un conjunto de etiquetas puede contener hasta 10 etiquetas, y también puede estar vacío. Si agrega una etiqueta a un recurso de Amazon DocumentDB con la misma clave que una etiqueta existente en el recurso, el nuevo valor sobrescribirá al antiguo.

AWS no aplica ningún significado semántico a las etiquetas, que se interpretan estrictamente como cadenas de caracteres. Amazon DocumentDB puede definir etiquetas en una instancia u otros recursos de Amazon DocumentDB, según la configuración utilizada al crear el recurso. Por ejemplo, Amazon DocumentDB podría añadir una etiqueta que indique que una instancia es para producción o para la realización de pruebas.

Puede añadir una etiqueta a una instantánea, pero la factura no reflejará esta agrupación.

Puede utilizar la Consola de administración de AWS o la AWS CLI para añadir, mostrar y eliminar etiquetas de los recursos de Amazon DocumentDB. Si utiliza la AWS CLI, deberá proporcionar el nombre de recurso de Amazon (ARN) correspondiente al recurso con el que desee trabajar. Para

obtener más información acerca de los ARN de Amazon DocumentDB, consulte Descripción de los nombres de recursos de Amazon DocumentDB () ARNs.

Restricciones de las etiquetas

Se aplican las siguientes restricciones de Amazon DocumentDB a las etiquetas:

- Cantidad máxima de etiquetas por recurso: 10
- Longitud máxima de la clave: 128 caracteres Unicode
- Longitud máxima del valor: 256 caracteres Unicode
- Caracteres válidos para la clave y valor: letras mayúsculas y minúsculas del juego de caracteres UTF-8, números, espacios y los siguientes caracteres: `_ . : / = + -` y `@` (expresión regular de Java: `"^([\\p{L}\\p{Z}\\p{N}_.:/=+\\-]*)$"`)
- Las claves y los valores de las etiquetas distinguen entre mayúsculas y minúsculas.
- El prefijo `aws:` no se puede usar para las claves o valores de una etiqueta; está reservado para AWS.

Agregación y actualización de etiquetas en un recurso de Amazon DocumentDB

Puede agregar hasta 10 etiquetas a un recurso mediante la Consola de administración de AWS o la AWS CLI.

Using the Consola de administración de AWS

El proceso para añadir una etiqueta a un recurso es similar independientemente de a qué recurso añada la etiqueta. En este ejemplo, se añade una etiqueta a un clúster.

Para añadir o actualizar etiquetas a un clúster utilizando la consola

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon DocumentDB en https://console.aws.amazon.com/docdb.
2. En el panel de navegación, seleccione clusters (clústeres).
3. Seleccione el nombre del clúster al que desea añadir etiquetas.
4. Desplácese hacia abajo hasta la sección Tags (Etiquetas) y, a continuación, elija Edit (Editar).
5. Para cada etiqueta que desee añadir a este recurso, haga lo siguiente:

a. Para añadir una nueva etiqueta, escriba el nombre de la etiqueta en el cuadro Key (Clave). Para cambiar el valor de una etiqueta, busque el nombre de la etiqueta en la columna Key (Clave).
b. Para asignar a la etiqueta un valor nuevo o actualizado, escriba un valor para la etiqueta en el cuadro Value (Valor).
c. Si desea añadir más etiquetas, elija Add (Añadir). En caso contrario, cuando haya terminado, elija Save (Guardar).

Using the AWS CLI

El proceso para añadir una etiqueta a un recurso es similar independientemente de a qué recurso añada etiquetas. En este ejemplo, se añaden tres etiquetas a un clúster. La segunda etiqueta, `key2`, no tiene ningún valor.

Utilice la operación AWS CLI de la `add-tags-to-resource` con estos parámetros.

Parámetros

- **`--resource-name`**: el ARN del recurso Amazon DocumentDB al que desea agregar etiquetas.
- **`--tags`**: una lista de etiquetas (par clave-valor) que desea agregar a este recurso en el formato. `Key=`*`key-name`*`,Value=`*`tag-value`*

Example

Para Linux, macOS o Unix:

```
aws docdb add-tags-to-resource \
    --resource-name arn:aws:rds:us-east-1:1234567890:cluster:sample-cluster \
    --tags Key=key1,Value=value1 Key=key2 Key=key3,Value=value3
```

Para Windows:

```
aws docdb add-tags-to-resource ^
    --resource-name arn:aws:rds:us-east-1:1234567890:cluster:sample-cluster \
    --tags Key=key1,Value=value1 Key=key2 Key=key3,Value=value3
```

La operación `add-tags-to-resource` no produce ningún resultado. Para ver los resultados de la operación, utilice la operación `list-tags-for-resource`.

Lista de etiquetas en un recurso de Amazon DocumentDB

Puede utilizar la Consola de administración de AWS o la AWS CLI para obtener una lista de las etiquetas de un recurso de Amazon DocumentDB.

Using the Consola de administración de AWS

El proceso para mostrar las etiquetas de un recurso es similar independientemente de a qué recurso añada la etiqueta. En este ejemplo, se muestran las etiquetas de un clúster.

Para mostrar las etiquetas en un clúster mediante la consola

1. Abra la consola de Amazon DocumentDB en https://console.aws.amazon.com/docdb.
2. En el panel de navegación, seleccione clusters (clústeres).
3. Seleccione el nombre del clúster para el que desea mostrar las etiquetas.
4. Para ver una lista de las etiquetas de este recurso, desplácese hacia abajo hasta la sección Tags (Etiquetas).

Using the AWS CLI

El proceso para mostrar las etiquetas de un recurso es similar independientemente del recurso cuyas etiquetas vaya a mostrar. En este ejemplo, se muestran las etiquetas de un clúster.

Utilice la operación AWS CLI de la `list-tags-for-resource` con estos parámetros.

Parámetros

- **`--resource-name`**: obligatorio. El ARN del recurso Amazon DocumentDB del que desea ver las etiquetas.

Example

Para Linux, macOS o Unix:

```
aws docdb list-tags-for-resource \
    --resource-name arn:aws:rds:us-east-1:1234567890:cluster:sample-cluster
```

Para Windows:

```
aws docdb list-tags-for-resource ^
    --resource-name arn:aws:rds:us-east-1:1234567890:cluster:sample-cluster
```

La salida de esta operación será similar a lo que se indica a continuación (formato JSON).

```
{
    "TagList": [
        {
            "Key": "key1",
            "Value": "value1"
        },
        {
            "Key": "key2",
            "Value": ""
        },
        {
            "Key": "key3",
            "Value": "value3"
        }
    ]
}
```

Eliminación de etiquetas de un recurso de Amazon DocumentDB

Puede usar la Consola de administración de AWS o la AWS CLI para eliminar etiquetas de recursos de Amazon DocumentDB.

Using the Consola de administración de AWS

El proceso para eliminar etiquetas de un recurso es similar independientemente del recurso que vaya a eliminar. En este ejemplo, se eliminan las etiquetas de un clúster.

Para eliminar las etiquetas de un clúster mediante la consola

1. Abra la consola de Amazon DocumentDB en https://console.aws.amazon.com/docdb.
2. En el panel de navegación, seleccione clusters (clústeres).
3. Seleccione el nombre del clúster cuyas etiquetas desea eliminar.
4. Desplácese hacia abajo hasta la sección Tags (Etiquetas) y, a continuación, elija Edit (Editar).

5. Si desea eliminar todas las etiquetas de este recurso, seleccione Remove all (Eliminar todas). De lo contrario, para cada etiqueta que desee eliminar de este recurso, haga lo siguiente:

   a. Localice el nombre de la etiqueta en la columna Key (Clave).

   b. Elija Remove (Eliminar) en la misma fila que la clave de etiqueta.

   c. Cuando termine, elija Guardar.

Using the AWS CLI

El proceso para eliminar una etiqueta de un recurso es similar independientemente del recurso del que vaya a eliminar una etiqueta. En este ejemplo, se elimina una etiqueta de un clúster.

Utilice la operación AWS CLI de la `remove-tags-from-resource` con estos parámetros.

- **`--resource-name`**: obligatorio. El ARN del recurso Amazon DocumentDB del que desea eliminar las etiquetas.
- **`--tag-keys`**: obligatorio. Una lista de las claves de etiqueta que desea quitar de este recurso.

Example

Para Linux, macOS o Unix:

```
aws docdb remove-tags-from-resource \
    --resource-name arn:aws:rds:us-east-1:1234567890:cluster:sample-cluster \
    --tag-keys key1 key3
```

Para Windows:

```
aws docdb remove-tags-from-resource ^
    --resource-name arn:aws:rds:us-east-1:1234567890:cluster:sample-cluster \
    --tag-keys key1 key3
```

La operación `removed-tags-from-resource` no produce ningún resultado. Para ver los resultados de la operación, utilice la operación `list-tags-for-resource`.

Mantenimiento de Amazon DocumentDB

Amazon DocumentDB realiza tareas de mantenimiento periódicas en los recursos de Amazon DocumentDB. En la mayoría de los casos, estas tareas de mantenimiento incluyen actualizaciones del motor de base de datos (mantenimiento de clústeres) o el sistema operativo subyacente de la instancia (mantenimiento de instancias). Las actualizaciones del motor de base de datos son parches necesarios e incluyen correcciones de seguridad, correcciones de errores y mejoras en el motor de base de datos. Si bien la mayoría de los parches del sistema operativo son opcionales, si no los aplica durante un tiempo, es posible que el parche sea necesario y se aplique automáticamente para mantener su postura de seguridad. Por lo tanto, le recomendamos que aplique las actualizaciones del sistema operativo a sus instancias de Amazon DocumentDB tan pronto como estén disponibles.

Los parches del motor de base de datos necesitan que desconecte los clústeres de Amazon DocumentDB durante un breve plazo de tiempo. Una vez disponibles, estos parches se programan automáticamente para que se apliquen durante un próximo periodo de mantenimiento programado del clúster de Amazon DocumentDB.

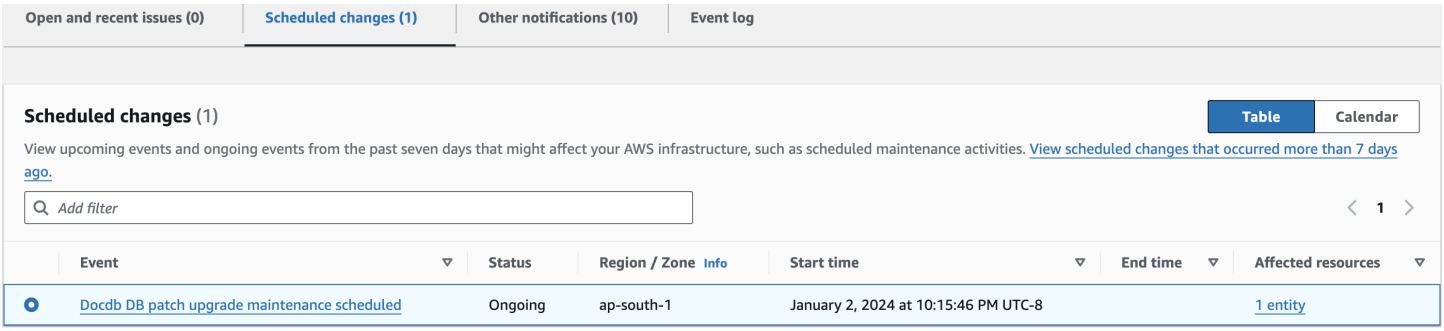
Los clústeres y las instancias tienen sus propios periodos de mantenimiento. Las modificaciones de la instancia y clúster que haya decidido no aplicar inmediatamente también se aplican durante el periodo de mantenimiento. De forma predeterminada, al crear un clúster, Amazon DocumentDB asigna un periodo de mantenimiento tanto para el clúster como para cada instancia individual. Puede elegir el periodo de mantenimiento en el momento de crear un clúster o una instancia. También puede modificar los periodos de mantenimiento en cualquier momento para ajustarlos a las prácticas o las programaciones de su empresa. Por lo general, se recomienda elegir periodos de mantenimiento que minimicen la repercusión de las tareas de mantenimiento en la aplicación (por ejemplo, por las noches o durante los fines de semana).

Temas

- Notificaciones de parches del motor de Amazon DocumentDB
- Visualización de las operaciones de mantenimiento pendientes de Amazon DocumentDB
- Actualizaciones del motor de Amazon DocumentDB
- Actualizaciones iniciadas por el usuario
- Administración de los periodos de mantenimiento de Amazon DocumentDB
- Actualizaciones del sistema operativo de Amazon DocumentDB

Notificaciones de parches del motor de Amazon DocumentDB

Recibirá notificaciones de mantenimiento de los parches del motor de base de datos necesarios mediante eventos de estado en la AWS consola Panel de estado (AHD) y mediante correos electrónicos. Cuando un parche de mantenimiento del motor de Amazon DocumentDB esté disponible en una AWS región concreta, todas las cuentas de usuario de Amazon DocumentDB afectadas de la región recibirán una notificación AHD y por correo electrónico para cada versión de Amazon DocumentDB afectada por el parche. Puede ver estas notificaciones en la sección de cambios programados del AHD de la consola. AWS La notificación incluirá detalles sobre el tiempo de disponibilidad de los parches, el calendario de aplicación automática, la lista de clústeres afectados y las notas de la versión. Esta notificación también se enviará por correo electrónico a la dirección de correo electrónico del usuario raíz de la AWS cuenta.



Una vez que reciba esta notificación, podrá optar por aplicar automáticamente estos parches del motor a los clústeres de Amazon DocumentDB antes de la fecha de aplicación automática programada. O bien, puede esperar a que los parches del motor se apliquen automáticamente durante un próximo periodo de mantenimiento (opción predeterminada).

> **Note**
>
> El Estado de la notificación en el AHD se establecerá como “En curso” hasta que se publique un nuevo parche del motor de Amazon DocumentDB con una nueva versión del parche del motor.
>
> Una vez aplicado el parche del motor al clúster de Amazon DocumentDB, la versión del parche del motor del clúster se actualizará para reflejar la versión en la notificación. Puede ejecutar el comando `db.runCommand({getEngineVersion: 1})` para verificar esta actualización.

AWS Health también se integra con Amazon EventBridge , que utiliza eventos para crear aplicaciones escalables basadas en eventos y se integra con más de 20 destinos AWS Lambda, incluidos Amazon Simple Queue Service (SQS) y otros. Puedes usar el código de `AWS_DOCDB_DB_PATCH_UPGRADE_MAINTENANCE_SCHEDULED` evento para configurar Amazon EventBridge antes de que los parches del motor estén disponibles. Puede configurarlo EventBridge para responder al evento y realizar automáticamente acciones, como capturar información sobre el evento, iniciar eventos adicionales, enviar notificaciones a través de canales adicionales, como notificaciones push AWS Console Mobile Application, y tomar medidas correctivas o de otro tipo, cuando un parche del motor Amazon DocumentDB esté disponible en su región.

En el raro caso de que Amazon DocumentDB cancele un parche del motor, recibirá una notificación de AHD y un correo electrónico en el que se le informará de la cancelación. En consecuencia, puedes usar el código de `AWS_DOCDB_DB_PATCH_UPGRADE_MAINTENANCE_CANCELLED` evento para configurar Amazon EventBridge para que responda a este evento. Consulta la Guía del EventBridge usuario de Amazon para obtener más información sobre el uso de EventBridge las reglas de Amazon.

Visualización de las operaciones de mantenimiento pendientes de Amazon DocumentDB

Puedes ver si hay una actualización de mantenimiento disponible para tu clúster utilizando el Consola de administración de AWS o el AWS CLI.

Si hay disponible una actualización, puede realizar una de las acciones siguientes:

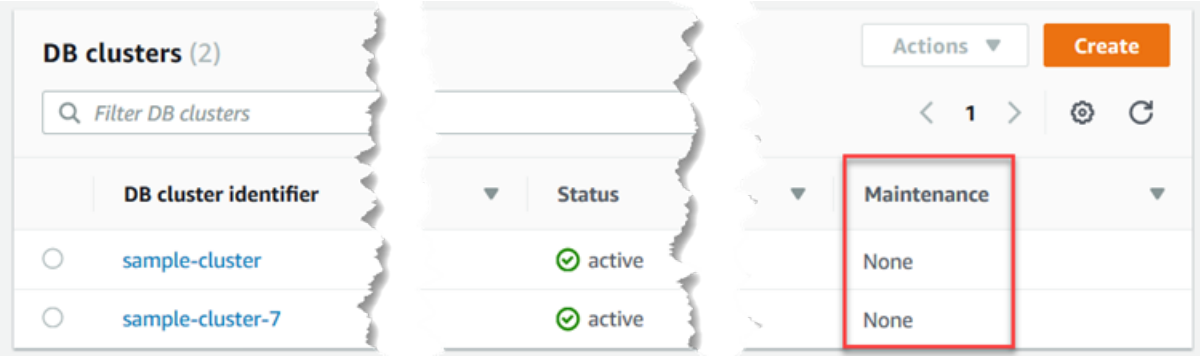
- Aplace una acción de mantenimiento que esté actualmente programada para el próximo periodo de mantenimiento (solo para los parches del sistema operativo).
- Aplicar inmediatamente las operaciones de mantenimiento.
- Programar las operaciones de mantenimiento para que se inicien durante el siguiente periodo de mantenimiento.

> **Note**
>
> Si no lleva a cabo ninguna acción, las acciones de mantenimiento necesarias, como los parches del motor, se aplicarán automáticamente en un próximo periodo de mantenimiento programado.

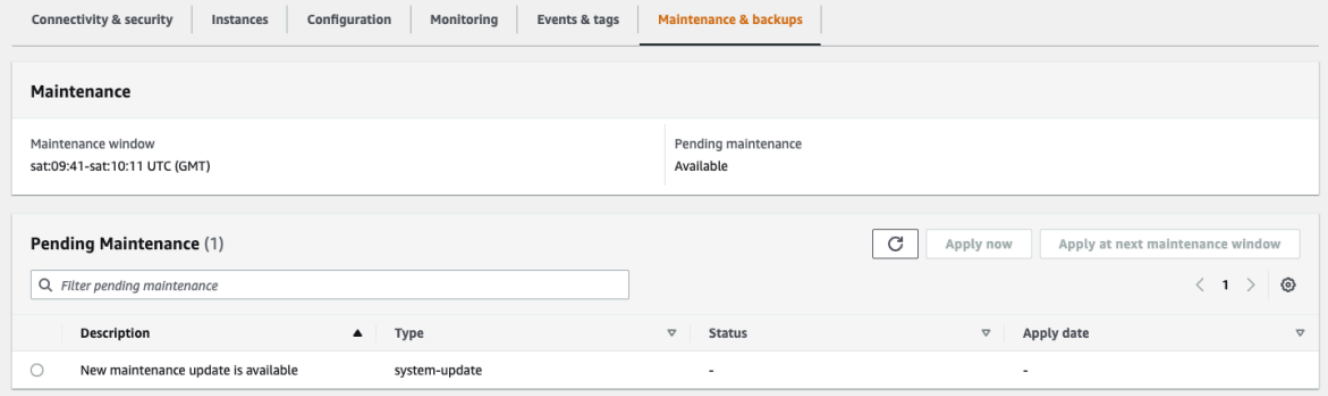
El periodo de mantenimiento determina el momento en que comienzan las operaciones pendientes, pero no limita su tiempo total de ejecución.

Using the Consola de administración de AWS

1. Inicie sesión en y abra la Consola de administración de AWS consola de Amazon DocumentDB en https://console.aws.amazon.com /docdb.
2. En el panel de navegación, seleccione Clusters (Clústeres).
3. Si hay disponible una actualización, se indicará con la palabra Disponible u Obligatorio, o Siguiente período en la columna Mantenimiento del clúster en la consola de Amazon DocumentDB, como se muestra a continuación:



4. Para realizar una acción, elija la instancia el clúster para mostrar sus detalles y, a continuación, seleccione Mantenimiento y copias de seguridad. Aparecerán los elementos de mantenimiento pendientes.



Using the AWS CLI

Utilice la siguiente AWS CLI operación para determinar qué acciones de mantenimiento están pendientes. Este resultado indica que no hay ninguna operación de mantenimiento pendiente.

```
aws docdb describe-pending-maintenance-actions
```

La salida de esta operación será similar a lo que se indica a continuación (formato JSON).

```
{
    "PendingMaintenanceActions": []
}
```

Actualizaciones del motor de Amazon DocumentDB

Con Amazon DocumentDB puede elegir el momento en que desea aplicar las operaciones de mantenimiento. Puede decidir cuándo Amazon DocumentDB aplica las actualizaciones mediante las Consola de administración de AWS teclas o. AWS CLI

Utilice los procedimientos que se explican en este tema para actualizar inmediatamente o para programar una actualización del clúster.

Using the Consola de administración de AWS

Puede utilizar la consola para administrar las actualizaciones de las instancias y los clústeres de Amazon DocumentDB.

Administración de la actualización de un clúster

1. Inicie sesión en y abra la Consola de administración de AWS consola de Amazon DocumentDB en https://console.aws.amazon.com /docdb.
2. En el panel de navegación, seleccione Clusters (Clústeres).
3. En la lista de clústeres, elija el botón situado junto al nombre del clúster al que desea aplicar la operación de mantenimiento.
4. En el menú Actions (Acciones), elija una de las opciones siguientes:
   - Upgrade now (Actualizar ahora) para realizar inmediatamente las tareas de mantenimiento pendientes.
   - Upgrade at next window (Actualizar en el siguiente periodo) para realizar las tareas de mantenimiento pendientes durante el siguiente periodo de mantenimiento del clúster.

También puede hacer clic en Aplicar ahora o Aplicar durante la próxima ventana de mantenimiento en la sección Mantenimiento pendiente de la pestaña Mantenimiento y copias de seguridad del clúster (consulte Uso de la Consola de administración de AWS en la sección anterior).

> **Note**
>
> Si no hay tareas de mantenimiento pendientes, las opciones anteriores están inactivas.

Using the AWS CLI

Para aplicar una actualización pendiente a un clúster, utilice la operación. `apply-pending-maintenance-action` AWS CLI

Parameters

- **`--resource-identifier`**: el Nombre de recurso de Amazon (ARN) Amazon DocumentDB del recurso al que se aplica la acción de mantenimiento pendiente.
- **`--apply-action`**: la acción de mantenimiento pendiente que se aplica a este recurso.

  Valores válidos: `system-update` y `db-upgrade`.
- **`--opt-in-type`**: un valor que indica el tipo de solicitud de alta o deshace una solicitud de alta. Una solicitud de alta de tipo `immediate` no se puede deshacer.

  Valores válidos:
  - `immediate`: aplicar inmediatamente la acción de mantenimiento.
  - `next-maintenance`: aplicar la acción de mantenimiento durante la siguiente ventana de mantenimiento del recurso.
  - `undo-opt-in`: cancelar todas las solicitudes de alta `next-maintenance` existentes.

Example

Para Linux, macOS o Unix:

```
aws docdb apply-pending-maintenance-action \
```

```
    --resource-identifier arn:aws:rds:us-east-1:123456789012:db:docdb \
    --apply-action system-update \
    --opt-in-type immediate
```

Para Windows:

```
aws docdb apply-pending-maintenance-action ^
    --resource-identifier arn:aws:rds:us-east-1:123456789012:db:docdb ^
    --apply-action system-update ^
    --opt-in-type immediate
```

Para devolver una lista de recursos que tienen al menos una actualización pendiente, utilice el `describe-pending-maintenance-actions` AWS CLI comando.

Example

Para Linux, macOS o Unix:

```
aws docdb describe-pending-maintenance-actions \
    --resource-identifier arn:aws:rds:us-east-1:001234567890:db:docdb
```

Para Windows:

```
aws docdb describe-pending-maintenance-actions ^
    --resource-identifier arn:aws:rds:us-east-1:001234567890:db:docdb
```

La salida de esta operación será similar a lo que se indica a continuación (formato JSON).

```
{
    "PendingMaintenanceActions": [
        {
            "ResourceIdentifier": "arn:aws:rds:us-
east-1:001234567890:cluster:sample-cluster",
            "PendingMaintenanceActionDetails": [
                {
                    "Action": "system-update",
                    "CurrentApplyDate": "2019-01-11T03:01:00Z",
                    "Description": "db-version-upgrade",
                    "ForcedApplyDate": "2019-01-18T03:01:00Z",
                    "AutoAppliedAfterDate": "2019-01-11T03:01:00Z"
                }
            ]
```

```
        }
    ]
}
```

También puede devolver una lista de recursos para un clúster especificando el `--filters` parámetro de la `describe-pending-maintenance-actions` AWS CLI operación. El formato de la operación `--filters` es `Name=`*`filter-name`*`,Values=`*`resource-id`*`,...`.

`db-cluster-id` son los valores aceptados para el parámetro `Name` del filtro. Este valor acepta una lista de identificadores de clúster o ARNs. La lista devuelta solo incluye las acciones de mantenimiento pendientes para los clústeres identificados por estos identificadores o. ARNs

En el ejemplo siguiente se obtienen las operaciones de mantenimiento pendientes para los clústeres `sample-cluster1` y `sample-cluster2`.

Example

Para Linux, macOS o Unix:

```
aws docdb describe-pending-maintenance-actions \
   --filters Name=db-cluster-id,Values=sample-cluster1,sample-cluster2
```

Para Windows:

```
aws docdb describe-pending-maintenance-actions ^
   --filters Name=db-cluster-id,Values=sample-cluster1,sample-cluster2
```

Fechas de aplicación

Cada operación de mantenimiento tiene una fecha de aplicación que encontrará al describir las operaciones de mantenimiento pendientes. Al leer el resultado de las acciones de mantenimiento pendientes del AWS CLI, aparecen tres fechas. Estos valores de fecha son `null` cuando el mantenimiento es opcional. Los valores se rellenan una vez que se programa o aplica la acción de mantenimiento correspondiente.

- **`CurrentApplyDate`**: fecha en la que se aplicará la acción de mantenimiento inmediatamente o en la siguiente ventana de mantenimiento.
- **`ForcedApplyDate`**: fecha en la que el mantenimiento se aplicará automáticamente, independientemente del período de mantenimiento.

- **`AutoAppliedAfterDate`**: fecha a partir de la cual se aplicará el mantenimiento durante el período de mantenimiento del clúster.

Actualizaciones iniciadas por el usuario

Como usuario de Amazon DocumentDB, puede iniciar las actualizaciones de los clústeres o las instancias. Por ejemplo, puede cambiar la clase de una instancia por otra con más o menos memoria o modificar el grupo de parámetros de un clúster. Amazon DocumentDB ve estos cambios de forma diferente a las actualizaciones iniciadas por Amazon DocumentDB. Para obtener más información sobre cómo modificar un clúster o una instancia, consulte lo siguiente:

- Modificación de un clúster de Amazon DocumentDB
- Modificación de una instancia de base de datos de Amazon DocumentDB

Para ver una lista de modificaciones pendientes iniciadas por el usuario, ejecute el siguiente comando.

Example

Para ver los cambios pendientes iniciados por el usuario para las instancias

Para Linux, macOS o Unix:

```
aws docdb describe-db-instances \
    --query 'DBInstances[*].
[DBClusterIdentifier,DBInstanceIdentifier,PendingModifiedValues]'
```

Para Windows:

```
aws docdb describe-db-instances ^
    --query 'DBInstances[*].
[DBClusterIdentifier,DBInstanceIdentifier,PendingModifiedValues]'
```

La salida de esta operación será similar a lo que se indica a continuación (formato JSON).

En este caso, `sample-cluster-instance` tiene un cambio pendiente en una clase de instancia `db.r5.xlarge`, mientras que `sample-cluster-instance-2` no tiene ningún cambio pendiente.

```
[
    [
```

```
        "sample-cluster",
        "sample-cluster-instance",
        {
            "DBInstanceClass": "db.r5.xlarge"
        }
    ],
    [
        "sample-cluster",
        "sample-cluster-instance-2",
        {}
    ]
]
```

Administración de los periodos de mantenimiento de Amazon DocumentDB

Cada instancia y clúster incluye un periodo de mantenimiento semanal durante el que se aplican los cambios pendientes. Este periodo de mantenimiento es una oportunidad de controlar cuándo se producen modificaciones y se aplican parches de software, en caso de que se solicite o sea necesario. Si hay un evento de mantenimiento programado para una semana determinada, se iniciará durante el periodo de mantenimiento de 30 minutos que identifique. La mayoría de los eventos de mantenimiento también se completan durante el periodo de mantenimiento de 30 minutos, aunque otros eventos de mantenimiento pueden tardar más de 30 minutos en completarse.

El periodo de mantenimiento de 30 minutos se selecciona al azar dentro de un bloque de 8 horas por región. Si no especifica un periodo de mantenimiento preferido al crear una instancia o un clúster, Amazon DocumentDB asigna un periodo de mantenimiento de 30 minutos un día de la semana seleccionado al azar.

En la siguiente tabla, se muestran los bloques de tiempo de cada región desde los que se asignan los periodos de mantenimiento predeterminados.

Nombre de la región	Region	Bloque de tiempo en UTC
Este de EE. UU. (Ohio)	us-east-2	03:00-11:00
Este de EE. UU. (Norte de Virginia)	us-east-1	03:00-11:00
Oeste de EE. UU. (Oregón)	us-west-2	06:00-14:00

Nombre de la región	Region	Bloque de tiempo en UTC
África (Ciudad del Cabo)	af-south-1	03:00-11:00
Asia-Pacífico (Hong Kong)	ap-east-1	06:00-14:00
Asia-Pacífico (Hyderabad)	ap-south-2	06:30–14:30
Asia-Pacífico (Malasia)	ap-southeast-5	13:00-21:00
Asia-Pacífico (Mumbai)	ap-south-1	06:00-14:00
Asia-Pacífico (Osaka)	ap-northeast-3	12:00–20:00
Asia-Pacífico (Seúl)	ap-northeast-2	13:00-21:00
Asia-Pacífico (Singapur)	ap-southeast-1	14:00–22:00
Asia-Pacífico (Sídney)	ap-southeast-2	12:00–20:00
Asia-Pacífico (Yakarta)	ap-southeast-3	08:00-16:00
Asia-Pacífico (Tailandia)	ap-southeast-7	15:00-23:00
Asia-Pacífico (Tokio)	ap-northeast-1	13:00-21:00
Canadá (centro)	ca-central-1	03:00-11:00
China (Pekín)	cn-north-1	06:00-14:00
China (Ningxia)	cn-northwest-1	06:00-14:00
Europa (Fráncfort)	eu-central-1	21:00-05:00
Europa (Irlanda)	eu-west-1	22:00-06:00
Europa (Londres)	eu-west-2	22:00-06:00
Europa (Milán)	eu-south-1	02:00-10:00
Europa (París)	eu-west-3	23:59-07:29

Nombre de la región	Region	Bloque de tiempo en UTC
Europa (España)	eu-south-2	02:00-10:00
Europa (Estocolmo)	eu-north-1	04:00 — 12:00
México (centro)	mx-central-1	03:00-11:00
Medio Oriente (EAU)	me-central-1	05:00-13:00
América del Sur (São Paulo)	sa-east-1	00:00-08:00
Israel (Tel Aviv)	il-central-1	04:00-12:00
AWS GovCloud (Este de EE. UU.)	us-gov-east-1	17:00-01:00
AWS GovCloud (Estados Unidos-Oeste)	us-gov-west-1	06:00-14:00

Cambio de los periodos de mantenimiento de Amazon DocumentDB

El periodo de mantenimiento debe corresponder al momento de mínimo uso y, por tanto, podría ser preciso modificarlo cada cierto tiempo. El clúster o la instancia solo dejan de estar disponibles durante este periodo si se están aplicando cambios en el sistema (por ejemplo, se está realizando una operación de escalado del almacenamiento o un cambio de clase de instancia) y se requiere una interrupción. En ese caso, solo dejará de estar disponible durante el tiempo mínimo requerido para realizar los cambios necesarios.

En el caso de las actualizaciones del motor de base de datos, Amazon DocumentDB utiliza el periodo de mantenimiento preferido del clúster y no el periodo de mantenimiento de las instancias individuales.

Para cambiar el periodo de mantenimiento

- Para un clúster, consulte Modificación de un clúster de Amazon DocumentDB.
- Para una instancia, consulte Modificación de una instancia de base de datos de Amazon DocumentDB.

Actualizaciones del sistema operativo de Amazon DocumentDB

En ocasiones, las instancias de los clústeres de Amazon DocumentDB requieren actualizaciones del sistema operativo. Amazon DocumentDB actualiza el sistema operativo a una versión más reciente para mejorar el rendimiento de la base de datos y la posición de seguridad general de los clientes. Las actualizaciones del sistema operativo no cambian la versión del motor del clúster ni la clase de instancia de una instancia de Amazon DocumentDB.

Le recomendamos que actualice primero las instancias del lector en un clúster y, a continuación, la instancia del escritor para maximizar la disponibilidad de su clúster. No recomendamos actualizar las instancias de lector y escritor al mismo tiempo, ya que podría producirse un tiempo de inactividad en caso de una conmutación por error.

La mayoría de las actualizaciones del sistema operativo para Amazon DocumentDB son opcionales y no tienen una fecha fija para aplicarlas. Sin embargo, si no aplica estas actualizaciones durante un tiempo, es posible que acaben siendo necesarias y se apliquen automáticamente durante el periodo de mantenimiento de la instancia. Esto ayuda a mantener la posición de seguridad de la base de datos. Para evitar cualquier tiempo de inactividad inesperado, le recomendamos que aplique las actualizaciones del sistema operativo a las instancias de Amazon DocumentDB tan pronto como estén disponibles y que establezca el periodo de mantenimiento de las instancias en el momento que le resulte más conveniente según las necesidades de la empresa.

Para recibir una notificación cuando haya una nueva actualización opcional disponible, puede suscribirse al RDS-EVENT-0230 en la categoría de eventos de parches de seguridad. Para obtener información sobre la suscripción a eventos de Amazon DocumentDB, consulte Suscripción a eventos de Amazon DocumentDB.

Debe esperar que, mientras se lleva a cabo el mantenimiento en el clúster o la instancia, si se trata de una instancia principal, se producirá una conmutación por error. Para mejorar su disponibilidad, le recomendamos que utilice más de una instancia para sus clústeres de Amazon DocumentDB. Para obtener más información, consulte Conmutación por error a Amazon DocumentDB.

> **Note**
>
> Para determinadas funciones de administración, Amazon DocumentDB utiliza tecnología operativa que se comparte con Amazon Relational Database Service (Amazon RDS).

> **Important**
>
> La instancia de Amazon DocumentDB se desconectará durante la actualización del sistema operativo. Puede minimizar el tiempo de inactividad del clúster si dispone de un clúster de varias instancias. Si no tiene un clúster de varias instancias, puede optar por crear uno temporalmente mediante la adición de instancias secundarias para llevar a cabo este mantenimiento y, a continuación, eliminar las instancias de lectura adicionales una vez finalizado el mantenimiento (se aplicarán los cargos habituales por la instancia secundaria).

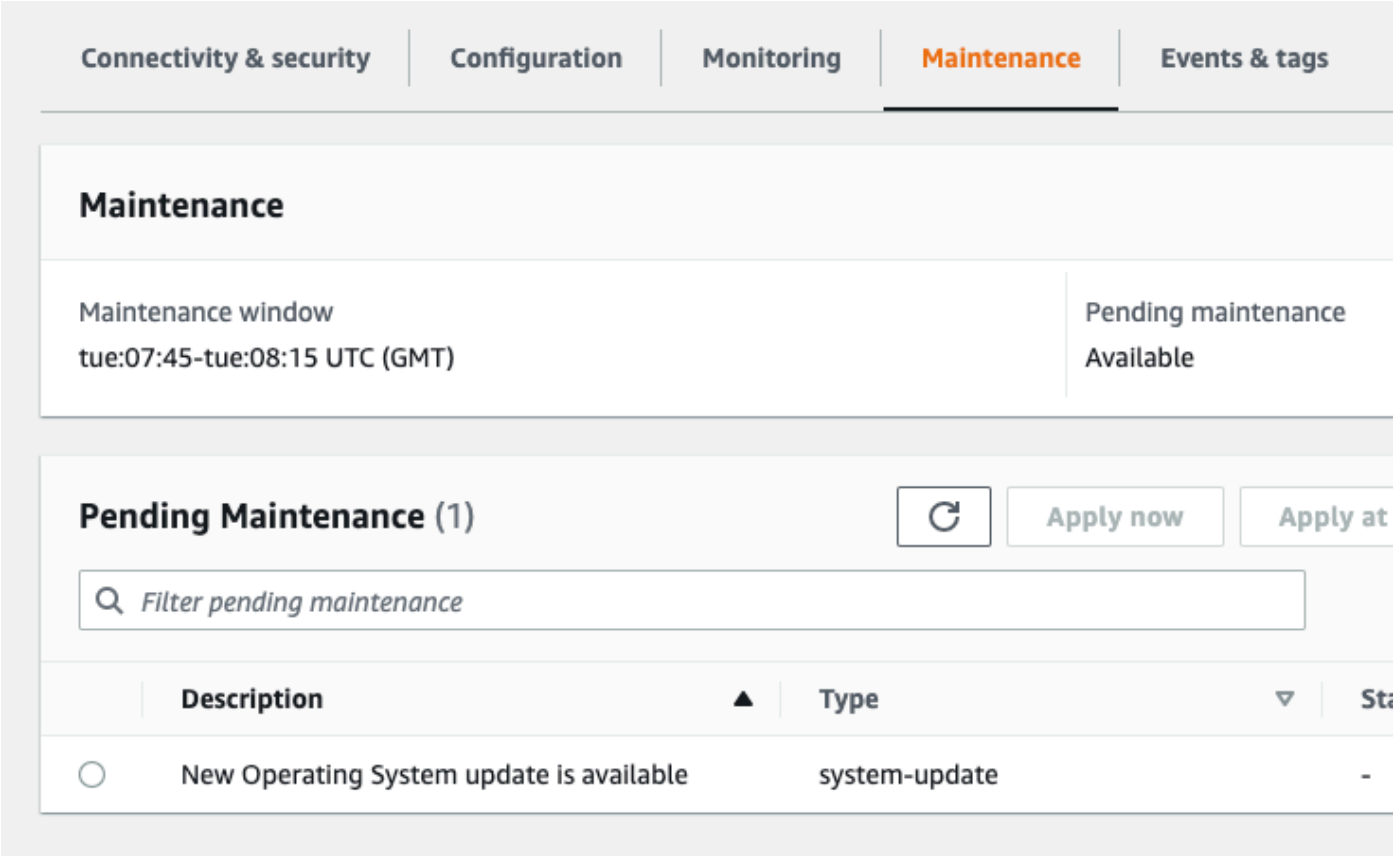
> **Note**
>
> Mantenerse al día en todas las actualizaciones opcionales y obligatorias podría ser necesario para cumplir varias obligaciones de conformidad. Le recomendamos que aplique todas las actualizaciones que Amazon DocumentDB pone a disposición de forma rutinaria durante los periodos de mantenimiento.

Puede utilizar el Consola de administración de AWS o el AWS CLI para determinar si hay una actualización disponible.

Using the Consola de administración de AWS

Para determinar si una actualización está disponible mediante la Consola de administración de AWS:

1. Inicie sesión en y abra la Consola de administración de AWS consola de Amazon DocumentDB en https://console.aws.amazon.com /docdb.
2. En el panel de navegación, elija Clústeres y, a continuación, seleccione la instancia.
3. Elija Mantenimiento.
4. En la sección Mantenimiento pendiente, busque la actualización del sistema operativo.



Puede seleccionar la actualización del sistema operativo y hacer clic en Aplicar ahora o en Aplicar durante la próxima ventana de mantenimiento en la sección Mantenimiento pendiente. Si el valor de mantenimiento es siguiente periodo, aplace los elementos de mantenimiento seleccionando aplazar actualización. No puede aplazar una acción de mantenimiento si ya se ha iniciado.

Como alternativa, puede elegir la instancia de una lista de clústeres. Para ello, haga clic en Clústeres en el panel de navegación y seleccione Aplicar ahora o Aplicar durante la próxima ventana de mantenimiento en el menú Acciones.

Using the AWS CLI

Para determinar si hay una actualización disponible mediante el AWS CLI, ejecute el comando: `describe-pending-maintenance-actions`

```
aws docdb describe-pending-maintenance-actions
```

```
{
  "ResourceIdentifier": "arn:aws:docdb:us-east-1:123456789012:db:mydb2",
  "PendingMaintenanceActionDetails": [
    {
```

```
      "Action": "system-update",
      "Description": "New Operating System update is available"
    }
  ]
}
```

Las actualizaciones del sistema operativo son específicas para la versión del motor de Amazon DocumentDB y la clase de instancia. Por lo tanto, las instancias de Amazon DocumentDB reciben o requieren actualizaciones en diferentes momentos. Cuando una actualización del sistema operativo está disponible para su instancia en función de su versión del motor y de la clase de instancia, la actualización aparece en la consola. También se puede ver ejecutando el AWS CLI `describe-pending-maintenance-actions` comando o llamando a la operación de la `DescribePendingMaintenanceActions` API.

Si no está ejecutando la última versión del parche de clúster del motor de Amazon DocumentDB, es posible que la actualización del sistema operativo no aparezca en la lista de mantenimiento disponible. Para ver y administrar la actualización del sistema operativo, primero debe actualizar a la versión más reciente de parche del motor.

Descripción de los roles vinculados a servicios

Amazon DocumentDB (compatible con MongoDB) usa AWS Identity and Access Management roles vinculados a servicios (IAM). Un rol vinculado a un servicio es un tipo único de rol de IAM que está vinculado directamente a Amazon DocumentDB. Amazon DocumentDB predefine las funciones vinculadas a servicios e incluyen todos los permisos que el servicio requiere para llamar a AWS otros servicios en su nombre.

Un rol vinculado a un servicio simplifica el uso de Amazon DocumentDB porque ya no tendrá que agregar manualmente los permisos requeridos. Amazon DocumentDB define los permisos de sus roles vinculados al servicio y, a menos que esté definido de otra manera, solo Amazon DocumentDB puede asumir sus roles. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se pueda asociar a ninguna otra entidad de IAM.

Las funciones se pueden eliminar únicamente después de eliminar primero sus recursos relacionados. De esta forma, se protegen los recursos de Amazon DocumentDB, ya que se evita que se puedan eliminar accidentalmente permisos de acceso a los recursos.

Para obtener información sobre otros servicios que son compatibles con los roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM y busque los servicios que muestran

Yes (Sí) en la columna Service-Linked Role (Rol vinculado a servicios). Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado al servicio en cuestión.

Permisos de roles vinculados a servicios para Amazon DocumentDB

Amazon DocumentDB (compatible con MongoDB) utiliza el rol vinculado a servicios denominado RDS para AWSServiceRoleForpermitir que Amazon DocumentDB llame a los servicios en nombre de sus clústeres. AWS

El rol vinculado al servicio AWSService RoleFor de RDS confía en los siguientes servicios para asumir el rol:

- `docdb.amazonaws.com`

La política de permisos del rol permite que Amazon DocumentDB realice las siguientes acciones en los recursos especificados:

- Acciones en `ec2`:
  - `AssignPrivateIpAddresses`
  - `AuthorizeSecurityGroupIngress`
  - `CreateNetworkInterface`
  - `CreateSecurityGroup`
  - `DeleteNetworkInterface`
  - `DeleteSecurityGroup`
  - `DescribeAvailabilityZones`
  - `DescribeInternetGateways`
  - `DescribeSecurityGroups`
  - `DescribeSubnets`
  - `DescribeVpcAttribute`
  - `DescribeVpcs`
  - `ModifyNetworkInterfaceAttribute`
  - `RevokeSecurityGroupIngress`
  - `UnassignPrivateIpAddresses`
- Acciones en `sns`:

  - `ListTopic`
  - `Publish`
- Acciones en `cloudwatch`:
  - `PutMetricData`
  - `GetMetricData`
  - `CreateLogStream`
  - `PullLogEvents`
  - `DescribeLogStreams`
  - `CreateLogGroup`

> **Note**
>
> Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Podría encontrarse con el siguiente mensaje de error:
> Unable to create the resource. Verify that you have permission to create service linked role. Otherwise wait and try again later.
> Si aparece este error, asegúrese de que tiene los siguientes permisos habilitados:
>
> ```
> {
>     "Action": "iam:CreateServiceLinkedRole",
>     "Effect": "Allow",
>     "Resource": "arn:aws:iam::*:role/aws-service-role/rds.amazonaws.com/
> AWSServiceRoleForRDS",
>     "Condition": {
>         "StringLike": {
>             "iam:AWSServiceName":"rds.amazonaws.com"
>         }
>     }
> }
> ```

Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Creación de un rol vinculado a servicios para Amazon DocumentDB

No necesita crear manualmente un rol vinculado a servicios. Al crear un clúster, Amazon DocumentDB se encarga de crear de nuevo el rol vinculado a servicios en su nombre.

Si elimina este rol vinculado a un servicio y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Al crear un clúster, Amazon DocumentDB se encarga de crear de nuevo el rol vinculado a servicios en su nombre de nuevo.

Modificación de un rol vinculado a servicios para Amazon DocumentDB

Amazon DocumentDB no le permite modificar la función vinculada al servicio de AWSService RoleFor RDS. Después de crear un rol vinculado a un servicio, no podrá cambiar el nombre del rol, ya que varias entidades podrían hacer referencia al mismo. Sin embargo, puede modificar la descripción del rol utilizando IAM. Para obtener más información, consulte Edición de un rol vinculado a servicios en la Guía del usuario de IAM.

Eliminación de un rol vinculado a servicios para Amazon DocumentDB

Si ya no necesita utilizar una característica o servicio que requiere un rol vinculado a servicios, recomendamos que elimine dicho rol. Así no tendrá una entidad no utilizada que no se supervise ni mantenga de forma activa. Sin embargo, debe eliminar todos los clústeres para poder eliminar el rol vinculado al servicio.

Limpieza de un rol vinculado a servicios para Amazon DocumentDB

Antes de poder utilizar IAM para eliminar un rol vinculado a un servicio, primero debe confirmar que dicho rol no tiene sesiones activas y eliminar los recursos que utiliza.

Para comprobar si el rol vinculado al servicio tiene una sesión activa mediante la consola

1. Inicie sesión en la consola de IAM Consola de administración de AWS y ábrala en. https://console.aws.amazon.com/iam/
2. En el panel de navegación de la consola de IAM, elija Funciones y, a continuación, elija el nombre (no la casilla de verificación) de la función de AWSServiceRoleForRDS.
3. En la página Resumen del rol seleccionado, seleccione la pestaña Asesor de acceso.
4. En la pestaña Access Advisor, revise la actividad reciente del rol vinculado al servicio.

> **Note**
>
> Si no está seguro de si Amazon DocumentDB utiliza el rol de AWSService RoleFor RDS, puede intentar eliminarlo. Si el servicio está utilizando el rol, este no podrá eliminarse y podrá ver las regiones en las que se está utilizando. Si el rol se está utilizando, debe esperar que la sesión finalice para poder eliminarlo. No se puede revocar la sesión de un rol vinculado a servicios.

Si desea eliminar el rol de AWSService RoleFor RDS, primero debe eliminar todas las instancias y clústeres. Para obtener información acerca de cómo eliminar instancias y clústeres, consulte los siguientes temas:

- Eliminación de una instancia de Amazon DocumentDB
- Eliminación de un clúster de Amazon DocumentDB

Regiones admitidas para los roles vinculados a servicios para Amazon DocumentDB

Amazon DocumentDB admite el uso de roles vinculados a servicios en todas las regiones en las que se encuentra disponible el servicio. Para obtener más información, consulte https://docs.aws.amazon.com/documentdb/latest/developerguide/regions-and-azs.html#regions-and-azs-availability.

Uso de flujos de cambios con Amazon DocumentDB

La función de flujos de cambios de Amazon DocumentDB (con compatibilidad con MongoDB) brinda una secuencia en orden cronológico de los eventos de actualización que se producen dentro de las colecciones de su clúster. Puede leer eventos de una secuencia de cambios para implementar muchos casos de uso diferentes, incluidos los siguientes:

- Notificación de cambio
- Búsqueda de texto completo con Amazon OpenSearch Service (OpenSearch Service)
- Análisis con Amazon Redshift

Las aplicaciones pueden usar los flujos de cambios para suscribirse a los cambios de datos en colecciones individuales. Los eventos de flujos de cambios se ordenan a medida que se producen en el clúster y se almacenan durante 3 horas (valor predeterminado) desde el momento de registro del evento. El período de retención se puede ampliar hasta 7 días utilizando el parámetro `change_stream_log_retention_duration`. Para modificar el período de retención del flujo de cambios, consulte Modificación de la duración de retención del registro del flujo de cambios.

Temas

- Operaciones admitidas
- Facturación
- Limitaciones
- Habilitación de flujos de cambios
- Ejemplo: uso de flujos de cambios con Python
- Búsqueda completa de documentos
- Reanudación de un flujo de cambios
- Reanudación de un flujo de cambios con startAtOperationTime
- Reanudación de un flujo de cambios con postBatchResumeToken
- Transacciones en flujos de cambios
- Modificación de la duración de la retención del registro de flujos de cambios
- Uso de flujos de cambios en instancias secundarias

Operaciones admitidas

Amazon DocumentDB admite las siguientes operaciones para flujos de cambio:

- Todos los eventos de cambio admitidos en la API `db.collection.watch()`, `db.watch()` y `client.watch()` de MongoDB.
- Búsqueda completa de documentos para actualizaciones.
- Etapas de agregación: `$match`, `$project`, `$redact`, `$addFields` y `$replaceRoot`.
- Reanudación de un flujo de cambios desde un token de reanudación
- Reanudación de un flujo de cambios a partir de una marca de tiempo mediante `startAtOperation` (aplicable a Amazon DocumentDB 4.0 y versiones posteriores)

Facturación

La característica de secuencias de cambios de Amazon DocumentDB está desactivada de forma predeterminada y no genera ningún cargo adicional hasta que se habilita y se utiliza. El uso de secuencias de cambios en un clúster conlleva costos adicionales de lectura y escritura de IOPS y almacenamiento. Puede utilizar la operación `modifyChangeStreams` de la API con el fin de habilitar esta característica para las colecciones del clúster. Para obtener más información acerca de los precios, consulte Precios de Amazon DocumentDB.

Limitaciones

Las secuencias de cambio tienen las siguientes limitaciones en Amazon DocumentDB:

- En Amazon DocumentDB 3.6. y Amazon DocumentDB 4.0, los flujos de cambios solo se pueden abrir desde una conexión a la instancia principal de un clúster de Amazon DocumentDB. Amazon DocumentDB 3.6 y Amazon DocumentDB 4.0 no admiten la lectura de flujos de cambios en una instancia de réplica. Al invocar la operación de la API `watch()`, debe especificar una preferencia de lectura `primary` para asegurarse de que todas las lecturas se dirigen a la instancia principal (consulte la sección Ejemplo).
- En Amazon DocumentDB 5.0, los flujos de cambios se pueden abrir tanto desde la instancia principal como desde la secundaria, incluidos los clústeres globales. Puede especificar una preferencia de lectura secundaria para redirigir los flujos de cambios a instancias secundarias. Consulte Uso de flujos de cambios en instancias secundarias para ver las limitaciones y prácticas recomendadas adicionales.
- Los eventos escritos en una secuencia de cambios de una colección están disponibles hasta 7 días (el valor predeterminado es 3 horas). Los datos de flujos de cambios se eliminan después del periodo de tiempo de conservación de los registros, aunque no se hayan realizado cambios.
- Una operación de escritura de larga duración en una colección como `updateMany` o `deleteMany` puede estancar temporalmente la escritura de eventos de secuencias de cambio hasta que se completa dicha operación de escritura de larga duración.
- Amazon DocumentDB no es compatible con el registro de operaciones de MongoDB (`oplog`).
- Con Amazon DocumentDB, debe habilitar explícitamente las secuencias de cambios en una colección determinada.
- Si el tamaño total de un evento de secuencias de cambios (incluidos los datos de cambio y el documento completo, si se solicita) es mayor que `16 MB`, el cliente experimentará un error de lectura en las secuencias de cambios.

- Actualmente, el controlador Ruby no es compatible al usar `db.watch()` y `client.watch()` con Amazon DocumentDB 3.6.
- El resultado del comando `updateDescription` en los flujos de cambios es diferente en Amazon DocumentDB que en MongoDB cuando el valor actualizado del campo es el mismo que el anterior:
  - Amazon DocumentDB no devuelve ningún campo en la salida `updateDescription` si el campo proporcionado está especificado en el comando `$set` y su valor objetivo ya es igual al valor de origen.
  - MongoDB devuelve el campo en la salida, incluso si el valor especificado es igual al valor actual.

Habilitación de flujos de cambios

Puede habilitar las secuencias de cambios de Amazon DocumentDB para todas las colecciones contenidas en una base de datos determinada o solamente para las colecciones seleccionadas. Los siguientes ejemplos muestran cómo habilitar las secuencias de cambios para diferentes casos de uso mediante el shell de mongo. Las cadenas vacías se tratan como comodines al especificar los nombres de las bases de datos y de las colecciones.

```
//Enable change streams for the collection "foo" in database "bar"
db.adminCommand({modifyChangeStreams: 1,
    database: "bar",
    collection: "foo",
    enable: true});
```

```
//Disable change streams on collection "foo" in database "bar"
db.adminCommand({modifyChangeStreams: 1,
    database: "bar",
    collection: "foo",
    enable: false});
```

```
//Enable change streams for all collections in database "bar"
db.adminCommand({modifyChangeStreams: 1,
    database: "bar",
    collection: "",
    enable: true});
```

```
//Enable change streams for all collections in all databases in a cluster
db.adminCommand({modifyChangeStreams: 1,
```

```
    database: "",
    collection: "",
    enable: true});
```

Las secuencias de cambios se habilitarán para una colección si se cumple alguna de las siguientes condiciones:

- Tanto la base de datos como la colección están habilitadas explícitamente.
- La base de datos que contiene la colección está habilitada.
- Todas las bases de datos están habilitadas.

La eliminación de una colección de una base de datos no deshabilita las secuencias de cambios para esa colección si la base de datos principal también tiene activadas las secuencias de cambios o si todas las bases de datos del clúster están habilitadas. Si se crea una nueva colección con el mismo nombre que la colección eliminada, las secuencias de cambios se habilitarán para esa colección.

Puede enumerar todas las secuencias de cambios habilitadas del clúster mediante la etapa de canalización de agregación `$listChangeStreams`. Todas las etapas de agregación admitidas por Amazon DocumentDB se pueden utilizar en la canalización para un procesamiento adicional. Si se deshabilita una colección que antes estaba habilitada, no aparecerá en la salida de `$listChangeStreams`.

```
//List all databases and collections with change streams enabled
cursor = new DBCommandCursor(db,
    db.runCommand(
        {aggregate: 1,
        pipeline: [{$listChangeStreams: 1}],
        cursor:{}}));
```

```
//List of all databases and collections with change streams enabled
{ "database" : "test", "collection" : "foo" }
{ "database" : "bar", "collection" : "" }
{ "database" : "", "collection" : "" }
```

```
//Determine if the database “bar” or collection “bar.foo” have change streams enabled
cursor = new DBCommandCursor(db,
  db.runCommand(
```

```
      {aggregate: 1,
       pipeline: [{$listChangeStreams: 1},
                  {$match: {$or: [{database: "bar", collection: "foo"},
                                  {database: "bar", collection: ""},
                                  {database: "", collection: ""}]}}
                 ],
      cursor:{}}));
```

Ejemplo: uso de flujos de cambios con Python

El siguiente es un ejemplo del uso de una secuencia de cambios de Amazon DocumentDB con Python a nivel de la colección.

```
import os
import sys
from pymongo import MongoClient, ReadPreference

username = "DocumentDBusername"
password = <Insert your password>

clusterendpoint = "DocumentDBClusterEndpoint”
client = MongoClient(clusterendpoint, username=username, password=password, tls='true',
 tlsCAFile='global-bundle.pem')

db = client['bar']

#While ‘Primary’ is the default read preference, here we give an example of
#how to specify the required read preference when reading the change streams
coll = db.get_collection('foo', read_preference=ReadPreference.PRIMARY)
#Create a stream object
stream = coll.watch()
#Write a new document to the collection to generate a change event
coll.insert_one({'x': 1})
#Read the next change event from the stream (if any)
print(stream.try_next())

"""
Expected Output:
{'_id': {'_data': '015daf94f600000002010000000200009025'},
'clusterTime': Timestamp(1571788022, 2),
'documentKey': {'_id': ObjectId('5daf94f6ea258751778163d6')},
'fullDocument': {'_id': ObjectId('5daf94f6ea258751778163d6'), 'x': 1},
'ns': {'coll': 'foo', 'db': 'bar'},
```

```
'operationType': 'insert'}
"""

#A subsequent attempt to read the next change event returns nothing, as there are no
 new changes
print(stream.try_next())

"""
Expected Output:
None
"""

#Generate a new change event by updating a document
result = coll.update_one({'x': 1}, {'$set': {'x': 2}})
print(stream.try_next())

"""
Expected Output:
{'_id': {'_data': '015daf99d40000000101000000100009025'},
'clusterTime': Timestamp(1571789268, 1),
'documentKey': {'_id': ObjectId('5daf9502ea258751778163d7')},
'ns': {'coll': 'foo', 'db': 'bar'},
'operationType': 'update',
'updateDescription': {'removedFields': [], 'updatedFields': {'x': 2}}}
"""
```

El siguiente es un ejemplo del uso de una secuencia de cambios de Amazon DocumentDB con Python a nivel de la base de datos.

```
import os
import sys
from pymongo import MongoClient

username = "DocumentDBusername"
password = <Insert your password>
clusterendpoint = "DocumentDBClusterEndpoint”
client = MongoClient(clusterendpoint, username=username, password=password, tls='true',
 tlsCAFile='global-bundle.pem')

db = client['bar']
#Create a stream object
stream = db.watch()
coll = db.get_collection('foo')
```

```
#Write a new document to the collection foo to generate a change event
coll.insert_one({'x': 1})

#Read the next change event from the stream (if any)
print(stream.try_next())

"""
Expected Output:
{'_id': {'_data': '015daf94f600000002010000000200009025'},
'clusterTime': Timestamp(1571788022, 2),
'documentKey': {'_id': ObjectId('5daf94f6ea258751778163d6')},
'fullDocument': {'_id': ObjectId('5daf94f6ea258751778163d6'), 'x': 1},
'ns': {'coll': 'foo', 'db': 'bar'},
'operationType': 'insert'}
"""
#A subsequent attempt to read the next change event returns nothing, as there are no
 new changes
print(stream.try_next())

"""
Expected Output:
None
"""

coll = db.get_collection('foo1')

#Write a new document to another collection to generate a change event
coll.insert_one({'x': 1})
print(stream.try_next())

"""
Expected Output: Since the change stream cursor was the database level you can see
 change events from different collections in the same database
{'_id': {'_data': '015daf94f600000002010000000200009025'},
'clusterTime': Timestamp(1571788022, 2),
'documentKey': {'_id': ObjectId('5daf94f6ea258751778163d6')},
'fullDocument': {'_id': ObjectId('5daf94f6ea258751778163d6'), 'x': 1},
'ns': {'coll': 'foo1', 'db': 'bar'},
'operationType': 'insert'}
"""
```

Búsqueda completa de documentos

El evento de cambio de actualización no incluye el documento completo; incluye tan solo el cambio realizado. Si su caso de uso requiere el documento completo afectado por una actualización, puede habilitar la búsqueda completa de documentos al abrir la secuencia.

El documento `fullDocument` de un evento de secuencias de cambios de actualización representa la versión más reciente del documento actualizado en el momento de la búsqueda de documentos. Si se han producido cambios entre la operación de actualización y la búsqueda de `fullDocument`, es posible que el documento `fullDocument` no represente el estado del documento en el momento de la actualización.

Para crear un objeto de flujo con la búsqueda de actualizaciones habilitada, use este ejemplo:

```
stream = coll.watch(full_document='updateLookup')

#Generate a new change event by updating a document
result = coll.update_one({'x': 2}, {'$set': {'x': 3}})

stream.try_next()
```

El resultado del objeto de flujo tendrá un aspecto similar a este:

```
{'_id': {'_data': '015daf9b7c000000101000000100009025'},
'clusterTime': Timestamp(1571789692, 1),
'documentKey': {'_id': ObjectId('5daf9502ea258751778163d7')},
'fullDocument': {'_id': ObjectId('5daf9502ea258751778163d7'), 'x': 3},
'ns': {'coll': 'foo', 'db': 'bar'},
'operationType': 'update',
'updateDescription': {'removedFields': [], 'updatedFields': {'x': 3}}}
```

Reanudación de un flujo de cambios

Puede reanudar una secuencia de cambios más tarde mediante un token de reanudación, que es igual al campo `_id` del último documento de evento de cambio recuperado.

```
import os
import sys
from pymongo import MongoClient

username = "DocumentDBusername"
```

```
password = <Insert your password>
clusterendpoint = "DocumentDBClusterEndpoint”
client = MongoClient(clusterendpoint, username=username, password=password, tls='true',
 tlsCAFile='global-bundle.pem', retryWrites='false')

db = client['bar']
coll = db.get_collection('foo')
#Create a stream object
stream = db.watch()
coll.update_one({'x': 1}, {'$set': {'x': 4}})
event = stream.try_next()
token = event['_id']
print(token)

"""
Output: This is the resume token that we will later us to resume the change stream
{'_data': '015daf9c5b0000000101000000100009025'}
"""
#Python provides a nice shortcut for getting a stream’s resume token
print(stream.resume_token)

"""
Output
{'_data': '015daf9c5b0000000101000000100009025'}
"""
#Generate a new change event by updating a document
result = coll.update_one({'x': 4}, {'$set': {'x': 5}})
#Generate another change event by inserting a document
result = coll.insert_one({'y': 5})
#Open a stream starting after the selected resume token
stream = db.watch(full_document='updateLookup', resume_after=token)
#Our first change event is the update with the specified _id
print(stream.try_next())

"""
#Output: Since we are resuming the change stream from the resume token, we will see all
 events after the first update operation. In our case, the change stream will resume
 from the update operation {x:5}

{'_id': {'_data': '015f7e8f0c0000000601000000006000fe038'},
'operationType': 'update',
'clusterTime': Timestamp(1602129676, 6),
'ns': {'db': 'bar', 'coll': 'foo'},
'documentKey': {'_id': ObjectId('5f7e8f0ac423bafbfd9adba2')},
```

```
'fullDocument': {'_id': ObjectId('5f7e8f0ac423bafbfd9adba2'), 'x': 5},
'updateDescription': {'updatedFields': {'x': 5}, 'removedFields': []}}
"""
#Followed by the insert
print(stream.try_next())

"""
#Output:
{'_id': {'_data': '015f7e8f0c0000000701000000007000fe038'},
'operationType': 'insert',
'clusterTime': Timestamp(1602129676, 7),
'ns': {'db': 'bar', 'coll': 'foo'},
'documentKey': {'_id': ObjectId('5f7e8f0cbf8c233ed577eb94')},
'fullDocument': {'_id': ObjectId('5f7e8f0cbf8c233ed577eb94'), 'y': 5}}
"""
```

Reanudación de un flujo de cambios con **`startAtOperationTime`**

Puede reanudar un flujo de cambios más adelante a partir de una marca de tiempo determinada utilizando `startAtOperationTime`.

> **Note**
>
> `startAtOperationTime` se puede utilizar en Amazon DocumentDB 4.0 y versiones posteriores. Cuando se utiliza `startAtOperationTime`, el cursor del flujo de cambios solo devolverá los cambios que se hayan producido en la marca de tiempo especificada o después de ella. Los comandos `startAtOperationTime` y `resumeAfter` se excluyen mutuamente y, por lo tanto, no se pueden usar juntos.

```
import os
import sys
from pymongo import MongoClient

username = "DocumentDBusername"
password = <Insert your password>
clusterendpoint = "DocumentDBClusterEndpoint”
client = MongoClient(clusterendpoint, username=username, password=password, tls='true',
 tlsCAFile='rds-root-ca-2020.pem',retryWrites='false')
db = client['bar']
coll = db.get_collection('foo')
```

```
#Create a stream object
stream = db.watch()
coll.update_one({'x': 1}, {'$set': {'x': 4}})
event = stream.try_next()
timestamp = event['clusterTime']
print(timestamp)
"""
Output
Timestamp(1602129114, 4)
"""
#Generate a new change event by updating a document
result = coll.update_one({'x': 4}, {'$set': {'x': 5}})
result = coll.insert_one({'y': 5})
#Generate another change event by inserting a document
#Open a stream starting after specified time stamp

stream = db.watch(start_at_operation_time=timestamp)
print(stream.try_next())

"""
#Output: Since we are resuming the change stream at the time stamp of our first update
 operation (x:4), the change stream cursor will point to that event
{'_id': {'_data': '015f7e941a0000000301000000003000fe038'},
'operationType': 'update',
'clusterTime': Timestamp(1602130970, 3),
'ns': {'db': 'bar', 'coll': 'foo'},
'documentKey': {'_id': ObjectId('5f7e9417c423bafbfd9adbb1')},
'updateDescription': {'updatedFields': {'x': 4}, 'removedFields': []}}
"""

print(stream.try_next())
"""
#Output: The second event will be the subsequent update operation (x:5)
{'_id': {'_data': '015f7e9502000000050100000005000fe038'},
'operationType': 'update',
'clusterTime': Timestamp(1602131202, 5),
'ns': {'db': 'bar', 'coll': 'foo'},
'documentKey': {'_id': ObjectId('5f7e94ffc423bafbfd9adbb2')},
'updateDescription': {'updatedFields': {'x': 5}, 'removedFields': []}}
"""

print(stream.try_next())

"""
```

```
#Output: And finally the last event will be the insert operation (y:5)
{'_id': {'_data': '015f7e9502000000060100000006000fe038'},
'operationType': 'insert',
'clusterTime': Timestamp(1602131202, 6),
'ns': {'db': 'bar', 'coll': 'foo'},
'documentKey': {'_id': ObjectId('5f7e95025c4a569e0f6dde92')},
'fullDocument': {'_id': ObjectId('5f7e95025c4a569e0f6dde92'), 'y': 5}}
"""
```

Reanudación de un flujo de cambios con **postBatchResumeToken**

El flujo de cambios de Amazon DocumentDB ahora devuelve un campo adicional denominado `postBatchResumeToken`. Este campo lo devuelven el comando `$changestream` y el comando `getMore`.

Ejemplo del comando `$changestream` en Python:

```
db.command({"aggregate": "sales", "pipeline": [{ "$changeStream": {}}], "cursor":
 {"batchSize": 1}})
```

Resultado previsto:

```
cursor" : {
   "firstBatch" : [ ],
   "postBatchResumeToken" : {"_data" : "0167c8cbe60000000004"},
   "id" : NumberLong("9660788144470"),
   "ns" : "test.sales"
}
```

Ejemplo del comando `getMore` en Python:

```
db.command({"getMore": NumberLong(<cursor id>), "collection": "sales", "batchSize":
 1 })
```

Resultado previsto

```
cursor" : {
   "nextBatch" : [ ],
   "postBatchResumeToken" : {"_data" : "0167c8cbe60000000004"},
```

```
    "id" : NumberLong("9660788144470"),
    "ns" : "test.sales"
}
```

El campo `postBatchResumeToken` se puede usar para abrir nuevos cursores del flujo de cambios en el campo `resumeAfter`, de forma similar a como se usa el token de reanudación.

Abra un flujo que comience después del `postBatchResumeToken` seleccionado:

```
post_batch_resume_token = output['cursor']['postBatchResumeToken']
stream = db.watch(full_document='updateLookup', resume_after=post_batch_resume_token)
```

A diferencia de un token de reanudación normal, que siempre corresponde a una entrada del registro de operaciones (oplog) que refleja un evento real, `postBatchResumeToken` corresponde a una entrada del oplog que el flujo de cambios ha escaneado en el servidor y que no es necesariamente un cambio coincidente.

Si intenta reanudar con un token de reanudación normal y antiguo, la base de datos tendrá que escanear todas las entradas del oplog situadas entre la fecha y hora especificada y la hora actual. Esto puede generar muchas consultas internas y cada subconsulta se escanea durante un breve período de tiempo. Esto provocará un aumento en el uso de la CPU y degradará el rendimiento de la base de datos. Si se reanuda con el último `postBatchResumeToken`, se omite el escaneo de entradas del oplog que no coincidan.

Transacciones en flujos de cambios

Los eventos de flujo de cambios no contendrán eventos de transacciones sin confirmar ni canceladas. Por ejemplo, si inicia una transacción con una operación de `INSERT` y una operación de `UPDATE`, y la operación de `INSERT` se realiza correctamente, pero no así la operación de `UPDATE`, la transacción se revertirá. Como esta transacción se ha revertido, tu flujo de cambios no contendrá ningún evento de esta transacción.

Modificación de la duración de la retención del registro de flujos de cambios

Puede modificar la duración de la retención del registro de secuencias de cambios para que esté comprendida entre 1 hora y 7 días utilizando la Consola de administración de AWS o la AWS CLI.

Using the Consola de administración de AWS

Modificación de la duración de la retención del registro de secuencias de cambios

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon DocumentDB en https://console.aws.amazon.com/docdb.
2. En el panel de navegación, seleccione Grupos de parámetros.

   > **Tip**
   >
   > Si no ve el panel de navegación del lado izquierdo de la pantalla, seleccione el icono de menú
   > (≡)
   > en la esquina superior izquierda de la página.

3. En el panel Parameter groups (Grupos de parámetros), elija el grupo de parámetros de clúster asociado a su clúster. Para identificar el grupo de parámetros de clúster asociado a su clúster, consulte Determinación del grupo de parámetros de un clúster de Amazon DocumentDB.
4. La página resultante muestra los parámetros y sus detalles correspondientes para el grupo de parámetros de su clúster. Seleccione el parámetro `change_stream_log_retention_duration`.
5. En la parte superior derecha de la página, elija Edit (Editar) para cambiar el valor del parámetro. El parámetro `change_stream_log_retention_duration` se puede modificar para que abarque entre 1 hora y 7 días.
6. Realice el cambio y, a continuación, elija Modify cluster parameter (Modificar parámetro de clúster) para guardar los cambios. Para descartar los cambios, selecciona Cancel (Cancelar).

Using the AWS CLI

Para modificar los parámetros de un grupo de parámetros de clúster `change_stream_log_retention_duration`, utilice la operación `modify-db-cluster-parameter-group` con los siguientes parámetros:

- **`--db-cluster-parameter-group-name`**: obligatorio. El nombre del grupo de parámetros de clúster que va a modificar. Para identificar el grupo de parámetros de clúster asociado

a su clúster, consulte Determinación del grupo de parámetros de un clúster de Amazon DocumentDB.

- **`--parameters`**: obligatorio. Los parámetros que está modificando. Cada entrada de parámetro debe incluir lo siguiente:
  - **`ParameterName`**: el nombre del grupo de parámetros de clúster que va a modificar. En este caso, es `change_stream_log_retention_duration`
  - **`ParameterValue`**: el valor nuevo de este parámetro de clúster.
  - **`ApplyMethod`**: cómo desea que se apliquen los cambios a este parámetro. Los valores permitidos son `immediate` y `pending-reboot`.

> **Note**
>
> Los parámetros con el `ApplyType` de `static` deben tener un `ApplyMethod` de `pending-reboot`.

1. Para cambiar los valores del parámetro `change_stream_log_retention_duration`, ejecute el siguiente comando y reemplace `parameter-value` por el valor que desea que tenga el parámetro.

   Para Linux, macOS o Unix:

   ```
   aws docdb modify-db-cluster-parameter-group \
       --db-cluster-parameter-group-name sample-parameter-group \
       --parameters
    "ParameterName=change_stream_log_retention_duration,ParameterValue=<parameter-
   value>,ApplyMethod=immediate"
   ```

   Para Windows:

   ```
   aws docdb modify-db-cluster-parameter-group ^
       --db-cluster-parameter-group-name sample-parameter-group ^
       --parameters
    "ParameterName=change_stream_log_retention_duration,ParameterValue=<parameter-
   value>,ApplyMethod=immediate"
   ```

   La salida de esta operación será similar a lo que se indica a continuación (formato JSON).

```
{
    "DBClusterParameterGroupName": "sample-parameter-group"
}
```

2. Espere al menos 5 minutos.
3. Enumere los valores de parámetros de `sample-parameter-group` para garantizar que se han realizado los cambios.

   Para Linux, macOS o Unix:

```
aws docdb describe-db-cluster-parameters \
    --db-cluster-parameter-group-name sample-parameter-group
```

   Para Windows:

```
aws docdb describe-db-cluster-parameters ^
    --db-cluster-parameter-group-name sample-parameter-group
```

   La salida de esta operación será similar a lo que se indica a continuación (formato JSON).

```
{
    "Parameters": [
        {
            "ParameterName": "audit_logs",
            "ParameterValue": "disabled",
            "Description": "Enables auditing on cluster.",
            "Source": "system",
            "ApplyType": "dynamic",
            "DataType": "string",
            "AllowedValues": "enabled,disabled",
            "IsModifiable": true,
            "ApplyMethod": "pending-reboot"
        },
        {
            "ParameterName": "change_stream_log_retention_duration",
            "ParameterValue": "12345",
            "Description": "Duration of time in seconds that the change stream
 log is retained and can be consumed.",
            "Source": "user",
            "ApplyType": "dynamic",
```

```
            "DataType": "integer",
            "AllowedValues": "3600-86400",
            "IsModifiable": true,
            "ApplyMethod": "immediate"
        }
    ]
}
```

> **Note**
>
> La retención del registro de flujos de cambios no eliminará los registros anteriores al `change_stream_log_retention_duration` valor configurado hasta que el tamaño del registro sea superior a (>) 51.200 MB.

Uso de flujos de cambios en instancias secundarias

Para empezar a utilizar el flujo de cambios en las instancias secundarias, abra el cursor del flujo de cambios con `readPreference` como instancia secundaria.

Puede abrir un cursor de flujo de cambios para observar los cambios en una colección específica o en todas las colecciones de un clúster o base de datos. Puede abrir un cursor de flujo de cambios en cualquier instancia de Amazon DocumentDB y recuperar documentos del flujo de cambios tanto de las instancias de escritura como de lectura. Puede compartir los tokens de flujo de cambios (por ejemplo, `resumeToken` o `startOperationTime`) entre distintos cursores del flujo de cambios abiertos en una instancia de escritura y lectura.

Ejemplo

```
import os
import sys
from pymongo import MongoClient, ReadPreference

username = "DocumentDBusername"
password = <Your password>

clusterendpoint = "DocumentDBClusterEndpoint"

client = MongoClient(clusterendpoint, username=username, password=password, tls='true',
 tlsCAFile='global-bundle.pem')
```

```
db = client['bar']

# Make sure to use SECONDARY to redirect cursor reads from secondary instances
coll = db.get_collection('foo', read_preference=ReadPreference.SECONDARY)

# Create a stream object on RO. The token needs to generated from PRIMARY.
stream = coll.watch(resumeAfter=token)

for event in stream:
   print(event)
```

Directrices y limitaciones para los flujos de cambios en las instancias secundarias

- Los eventos del flujo de cambios deben replicarse desde la instancia principal a las instancias secundarias. Puede supervisar el retraso de la métrica `DBInstanceReplicaLag` en Amazon CloudWatch.
- Es posible que las marcas de tiempo de las instancias secundarias no estén siempre sincronizadas con las de la instancia principal. En este caso, espere retrasos en la marca de tiempo de la instancia secundaria para que pueda ponerse al día. Es recomendable que utilice `startAtOperationTime` o `resumeToken` para iniciar el reloj en la instancia secundaria.
- Es posible que obtenga un rendimiento inferior en las instancias secundarias en comparación con la instancia principal si el tamaño del documento es grande; está haciendo `fullDocumentLookup` y hay una gran carga de trabajo de escritura simultánea en la instancia principal. Como práctica recomendada, le recomendamos que supervise la proporción de aciertos de la caché del búfer en la secundaria y que se asegure de que la tasa de aciertos de la caché del búfer sea alta.

Uso de la intercalación en Amazon DocumentDB 8.0

Amazon DocumentDB 8.0 ahora admite la intercalación. La intercalación le permite configurar reglas específicas del idioma para la comparación de cadenas. Con la intercalación, puede especificar reglas para las comparaciones que distingan mayúsculas de minúsculas o especificar una configuración regional de idioma. La intercalación se puede configurar a nivel de colección o de índice en DocumentDB 8.0. Cuando se utiliza la intercalación en DocumentDB, internamente se crea un documento de intercalación con los siguientes parámetros.

```
{
locale: string,
caseLevel: boolean,
caseFirst: string,
strength: int,
numericOrdering: boolean,
alternate: string,
maxVariable: string,
backwards: boolean,
normalization: boolean
}
```

Limitaciones

La intercalación tiene las siguientes limitaciones en Amazon DocumentDB:

- La intercalación es compatible con el planificador v3 disponible en Amazon DocumentDB 8.0. El cambio a plannerv2 o plannerv1 puede provocar comportamientos incoherentes, incluidos errores de tipo «índice no encontrado».
- Debido a las diferencias inherentes a las bibliotecas, si se exporta una colección de mongodb con intercalación, tendrá que actualizar los archivos.bson de metadatos y cambiar su versión de 57.1 a 60.2 antes de realizar la migración.
- En raras ocasiones, la configuración de intercalación puede superar el límite interno de número de caracteres y provocar el siguiente error. «Error: el documento de intercalación tiene más atributos no predeterminados de los admitidos. Reduzca el número de opciones». En este caso, intente reducir las opciones que proporciona en el documento de cotejo o, si lo prefiere, puede intentar utilizar los valores predeterminados siempre que sea posible.

Uso de vistas en Amazon DocumentDB 8.0

- Amazon DocumentDB 8.0 ahora admite vistas. Las vistas funcionan como colecciones virtuales que presentan datos en función de operaciones de agregación especificadas. Al crear una vista, se define una consulta que transforma los datos de una o más colecciones de fuentes. Amazon DocumentDB 8.0 ejecuta esta consulta cada vez que se accede a la vista, sin consumir recursos de almacenamiento adicionales. A diferencia de las colecciones estándar, las vistas de Amazon DocumentDB 8.0 no almacenan los documentos en disco, lo que las convierte en una solución eficaz para presentar datos transformados o filtrados a las aplicaciones. Para crear una vista en

Amazon DocumentDB, puede utilizar el comando CreateView o el método auxiliar db.createView ():

```
db.createView("viewName","sourceCollection",
[
    { $match: { status: "active" } },
    { $project: { _id: 1, name: 1, email: 1 } }
]
)
```

Esto crea una vista denominada «viewName» basada en «SourceCollection» que solo incluye los documentos activos y proyecta únicamente los campos _id, name y correo electrónico. Las vistas de Amazon DocumentDB son de solo lectura. Las operaciones de escritura en las vistas devolverán un error. Para obtener un rendimiento óptimo con conjuntos de datos de gran tamaño, puede estructurar sus canalizaciones de visualización para maximizar la eficiencia. Para los procesos de agregación complejos, se recomienda utilizar la etapa $match como primera etapa o al principio del proceso para reducir la cantidad de documentos que deben procesarse las etapas posteriores y, de este modo, mejorar el rendimiento de las consultas.

Prácticas recomendadas

A continuación se detallan algunas de las prácticas recomendadas que se deben seguir con Views.

- Filtrar anticipadamente: utilice las etapas de $match al principio de las canalizaciones de visualización para reducir la cantidad de datos procesados.
- Evite las agregaciones complejas: para las vistas con agregaciones complejas a las que se accede con frecuencia, considere la posibilidad de crear una colección independiente con resultados precalculados que se actualicen periódicamente.
- Planificación de índices: asegúrese de que los campos utilizados en las canalizaciones de vistas, especialmente en las operaciones $match y $sort, estén indexados correctamente en la colección de origen.
- Optimización de consultas: utilice el comando explain para comprender cómo se ejecutan las consultas de visualización y optimizarlas en consecuencia.
- Alternativas para las vistas: dadas las diferencias funcionales entre las vistas de Amazon DocumentDB y MongoDB, considere la posibilidad de utilizar colecciones regulares con actualizaciones programadas como alternativa a las vistas cuando se encuentre con limitaciones.

Compatibilidad con los operadores de agregadores

Amazon DocumentDB admite muchos operadores de agregación en las definiciones de vistas y, al mismo tiempo, sigue ampliando la compatibilidad. Cuando utilice vistas, concéntrese en los siguientes operadores compatibles:

- $match para filtrar documentos
- $project para la selección y transformación de campos
- $addFields para añadir campos calculados
- $sort para ordenar los resultados
- $limit y $skip para paginación

Algunos operadores especializados, como $currentOp, $replaceRoot y $geoNear, actualmente funcionan en consultas de agregación directa en lugar de ver definiciones.

Aprovechamiento de índices y vistas

Las vistas de Amazon DocumentDB 8.0 utilizan los índices de la colección subyacente. Como resultado, no puede crear, eliminar ni reconstruir índices directamente en una vista. Sin embargo, unos índices bien diseñados en la colección fuente pueden mejorar considerablemente el rendimiento de las consultas de visualización. A continuación, se indican algunos pasos para optimizar el rendimiento de las consultas en las vistas:

- Asegúrese de que existan los índices adecuados en los campos de la colección fuente utilizados en la canalización de la vista, especialmente en las operaciones $match y $sort
- Utilice el método explain () para analizar los planes de ejecución de las consultas y verificar el uso de los índices. Por ejemplo, `db.viewName.find({...}).explain()`

Uso de AWS Lambda con flujos de cambios

Amazon DocumentDB está integrado con AWS Lambda de modo que pueda utilizar funciones de Lambda para procesar registros en un flujo de cambios. La asignación de orígenes de eventos de Lambda es un recurso que se puede utilizar para invocar funciones de Lambda con el fin de procesar eventos de Amazon DocumentDB que no invocan directamente Lambda. Con el flujo de cambios de Amazon DocumentDB como origen de eventos, puede crear aplicaciones basadas en eventos

que respondan a cambios en sus datos. Por ejemplo, puede utilizar funciones de Lambda para procesar documentos nuevos, realizar un seguimiento de actualizaciones de documentos existentes o registrar documentos eliminados.

Puede configurar una asignación de orígenes de eventos para enviar registros desde su flujo de cambios de Amazon DocumentDB a una función de Lambda. Los eventos pueden enviarse de uno en uno o por lotes para mejorar la eficiencia y se procesan por orden. Puede configurar el comportamiento de procesamiento de su asignación de orígenes de eventos en función de una duración específica (de 0 a 300 segundos) o del recuento de registros por lotes (límite máximo de 10 000 registros). Puede crear varios mapeos de fuentes de eventos para procesar los mismos datos con distintas funciones de Lambda o para procesar distintos elementos de varios flujos con una sola función.

Sin embargo, si la función devuelve un error, Lambda vuelve a intentar ejecutar el lote hasta que se procese correctamente. En caso de que los eventos del flujo de cambios hayan caducado, Lambda deshabilitará la asignación de orígenes de eventos. En este caso, puede crear una nueva asignación de orígenes de eventos y configurarla con la posición inicial que elija. Las asignaciones de orígenes de eventos Lambda procesan los eventos al menos una vez debido a la naturaleza distribuida de los sondeadores. Como resultado, la función de Lambda puede recibir eventos duplicados en situaciones excepcionales. Siga las mejores prácticas al trabajar con funciones AWS Lambda para crear funciones idempotentes para evitar problemas relacionados con eventos duplicados. Para obtener más información, consulte Uso de AWS Lambda console con Amazon DocumentDB en la Guía para desarrolladores de AWS Lambda.

Como práctica recomendada de rendimiento, la función Lambda debe ser de corta duración. Para evitar introducir retrasos innecesarios en el procesamiento, tampoco debe ejecutar una lógica compleja. Para un flujo de alta velocidad en concreto, es mejor desencadenar un flujo de trabajo asíncrono de funciones de posprocesamiento que funciones Lambda sincrónicas de larga duración. Para obtener más información sobre AWS Lambda, consulte la Guía para desarrolladores de AWS Lambda.

Limitaciones

A continuación, se describen las limitaciones que se deben tener en cuenta al trabajar con Amazon DocumentDB y AWS Lambda:

- AWS Lambda solo es compatible actualmente con Amazon DocumentDB 4.0 y 5.0.
- AWS Lambda no es compatible actualmente con clústeres elásticos ni clústeres globales.

- Los tamaños de carga útil de AWS Lambda no pueden superar los 6 MB. Para obtener más información sobre los tamaños de los lotes de Lambda, consulte “Comportamiento de procesamiento por lotes” en la sección Asignación de origen de eventos de Lambda de la Guía para desarrolladores de AWS Lambda.

Uso de Amazon DocumentDB Elastic Clusters

Los clústeres elásticos de Amazon DocumentDB admiten cargas de trabajo con millones de reads/writes petabytes de capacidad de almacenamiento por segundo. Los clústeres elásticos también simplifican la forma en que los desarrolladores interactúan con Amazon DocumentDB al eliminar la necesidad de elegir, administrar o actualizar instancias.

Los Amazon DocumentDB Elastic Clusters fueron creados para:

- Proporcionar una solución para los clientes que buscan una base de datos que ofrezca una escala prácticamente ilimitada con amplias capacidades de consulta y compatibilidad con la API de MongoDB.
- Ofrecer a los clientes límites de conexión más altos y reducir el tiempo de inactividad provocado por la aplicación de parches.
- Seguir invirtiendo en una arquitectura nativa en la nube, elástica y líder en su clase para las cargas de trabajo de JSON.

Temas

- Casos de uso de clústeres elásticos
- Ventajas de los clústeres elásticos
- Disponibilidad en regiones y versiones de clústeres elásticos
- Limitaciones
- Clústeres elásticos de Amazon DocumentDB: cómo funcionan
- Introducción a los clústeres elásticos de Amazon DocumentDB
- Prácticas recomendadas para los clústeres elásticos de Amazon DocumentDB
- Administración de los clústeres elásticos de Amazon DocumentDB
- Activación del cifrado de datos en reposo de un clúster elástico de Amazon DocumentDB
- Roles vinculados a servicios en clústeres elásticos

Casos de uso de clústeres elásticos

Las bases de datos documentales son útiles para cargas de trabajo que requieren un esquema flexible que permita un desarrollo rápido e iterativo. Para ver ejemplos de casos de uso de Amazon DocumentDB, consulte Casos de uso de bases de datos de documentos.

A continuación, se incluyen algunos ejemplos de casos de uso para los que los clúster de elasticidad puedan ofrecer importantes ventajas:

Perfiles de usuario

Como las bases de datos documentales tienen un esquema flexible, pueden almacenar documentos que tengan atributos y valores de datos diferentes a escala. Los clúster elásticos son una solución práctica para los perfiles online en los que diferentes usuarios proporcionan diferentes tipos de información. Suponga que sus aplicaciones admiten cientos de millones de perfiles de usuario. Para admitir dichas aplicaciones puede usar clústeres elásticos, ya que se pueden ampliar y reducir para soportar millones de escrituras y lecturas en estos perfiles de usuario. También puede reducir verticalmente de cara a las horas de menor actividad para disminuir los costos.

Administración de contenido y registros históricos

Para administrar eficazmente el contenido, debe poder recopilar y agrupar contenido de una variedad de orígenes y enviárselo al cliente. Debido a su esquema flexible, las bases de datos documentales son perfectas para recopilar y almacenar cualquier tipo de datos. Puede utilizarlas para crear e incorporar nuevos tipos de contenido, incluido el contenido generado por el usuario, como imágenes, comentarios, y vídeos. Con el tiempo, es posible que su base de datos requiera más espacio de almacenamiento. Con los clústeres elásticos, puede distribuir sus datos entre más volúmenes de almacenamiento, lo que le permite almacenar petabytes de datos en un solo clúster.

Ventajas de los clústeres elásticos

AWS integración de servicios

Los clústeres elásticos de Amazon DocumentDB se integran con otros AWS servicios de la misma manera que lo hace Amazon DocumentDB:

- Migración: puede usar AWS Database Migration Service (DMS) para migrar de MongoDB y otras bases de datos relacionales a clústeres elásticos de Amazon DocumentDB.

- Supervisión: puede supervisar el estado y el rendimiento de su clúster elástico mediante Amazon CloudWatch.
- Seguridad: puede configurar la autenticación y la autorización mediante AWS Identity and Access Management (IAM) para administrar los recursos de su clúster elástico, como la creación y actualización de un clúster elástico, y usar Amazon VPC para conexiones seguras solo de VPC. No se admite el inicio de sesión mediante autenticación de IAM para los clústeres elásticos.
- Administración de datos: puede utilizar from/to otros AWS servicios AWS Glue para importar y exportar datos, como Amazon S3, Amazon Redshift y Amazon OpenSearch Service.

Disponibilidad en regiones y versiones de clústeres elásticos

Disponibilidad regional para clústeres elásticos

La siguiente tabla muestra AWS las regiones en las que están disponibles actualmente los clústeres elásticos de Amazon DocumentDB y el punto final de cada región.

Nombre de la región	Region	Zonas de disponibilidad
Este de EE. UU. (Norte de Virginia)	`us-east-1`	5
Este de EE. UU. (Ohio)	`us-east-2`	3
Oeste de EE. UU. (Oregón)	`us-west-2`	3
Asia-Pacífico (Hong Kong)	`ap-east-1`	3
Asia-Pacífico (Bombay)	`ap-south-1`	3
Asia-Pacífico (Seúl)	`ap-northeast-2`	3
Asia-Pacífico (Singapur)	`ap-southeast-1`	3
Asia-Pacífico (Sídney)	`ap-southeast-2`	3
Asia-Pacífico (Tokio)	`ap-northeast-1`	3
Canadá (centro)	`ca-central-1`	3

Nombre de la región	Region	Zonas de disponibilidad
América del Sur (São Paulo)	`sa-east-1`	3
Europa (Fráncfort)	`eu-central-1`	3
Europa (Irlanda)	`eu-west-1`	3
Europa (Londres)	`eu-west-2`	3
Europa (Milán)	`eu-south-1`	3
Europa (París)	`eu-west-3`	3

Disponibilidad de versiones

Los clústeres elásticos admiten el protocolo Wire compatible con MongoDB 5.0. Para ver las diferencias entre los clústeres basados en instancias de Amazon DocumentDB 4.0 y los clústeres elásticos, consulte Diferencias funcionales entre Amazon DocumentDB 4.0 y los clústeres elásticos. Nota: Los clústeres elásticos no son compatibles con Amazon DocumentDB 8.0

Limitaciones

Administración de clústeres elásticos

Esta versión no admite las siguientes funciones y capacidades de administración de clústeres:

- Puerto personalizado (solo se admite el 27017)
- Capacidad de usar los usuarios y roles de IAM para la autenticación en la base de datos
- Capacidad para crear clústeres globales
- Eventos de Amazon DocumentDB existentes y suscripción a eventos
- Partición por rangos
- Partición de colección existente
- Clave de partición de varios campos
- Cambio de la clave de partición
- Point-in-time restaurar

- Clonación
- Información de rendimiento

> **Note**
>
> Para obtener información sobre los límites de los clústeres elásticos, consulte Cuotas y límites de Amazon DocumentDB.

Operaciones de consulta y escritura

Los siguientes comandos y capacidades de las operaciones de consulta y escritura no se admiten en esta versión:

- Comandos DDL durante las operaciones de escalado
- Profiler
- Grupos de parámetros
- AWS Config
- AWS Backup

Gestión de colecciones e índices

Esta versión no admite las siguientes funciones y capacidades de índices y colecciones:

- Índices únicos
- Índices parciales
- Índices de texto
- Índices vectoriales
- Compresión de documentos

Administración y diagnóstico

Esta versión no admite los siguientes comandos y capacidades de administración y diagnóstico:

- AWS Secrets Manager

- Role-based-access-control roles personalizados (RBAC).
- Al conectarse, no se admite Write Concern con un valor de 0.
- Cambio de subredes pertenecientes a una VPC que actualmente no está asignada a un clúster elástico existente.

Características de suscripción

Esta versión no admite las siguientes características opcionales de Amazon DocumentDB:

- Transacciones ACID
- Auditoría de DDL/DML
- Change streams
- Comandos de sesión

Clústeres elásticos de Amazon DocumentDB: cómo funcionan

En los temas de esta sección se observa información acerca de los mecanismos y funciones que impulsan los clústeres elásticos de Amazon DocumentDB.

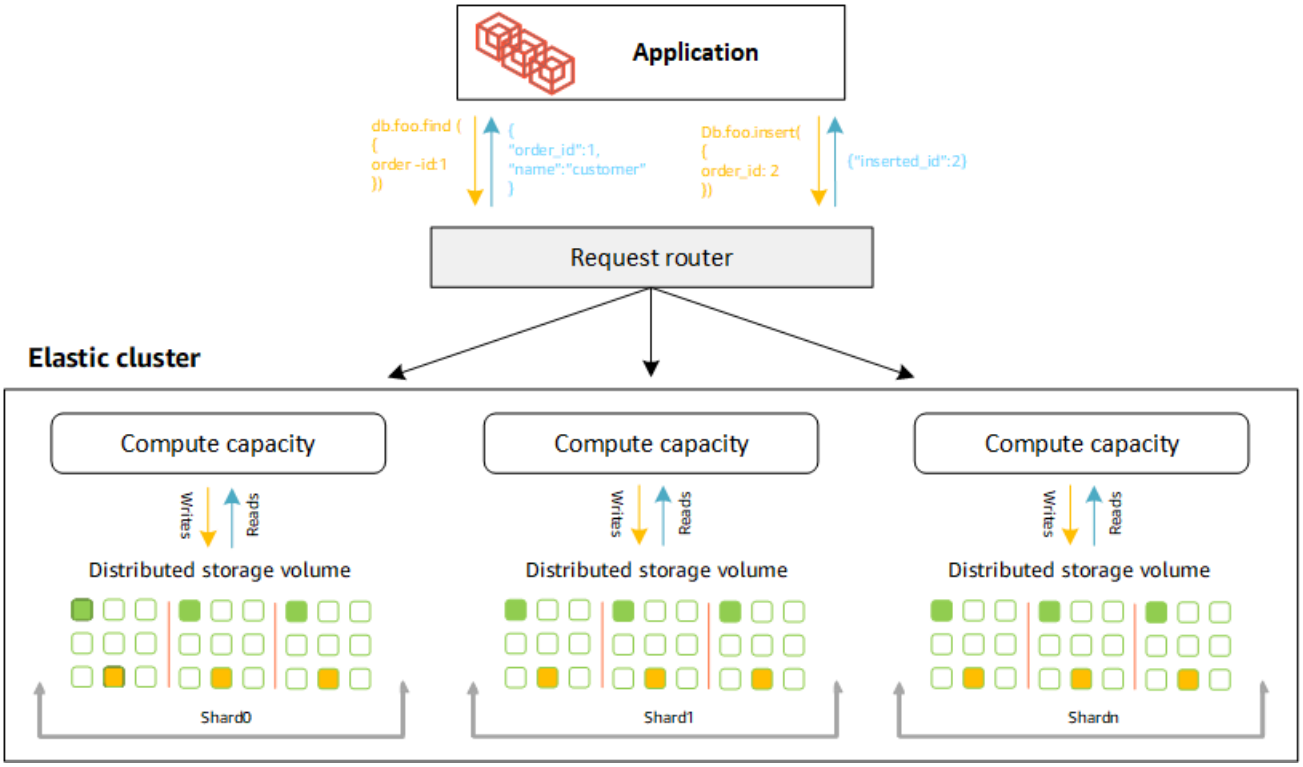
Temas

- Partición en los clústeres elásticos de Amazon DocumentDB
- Migración de clústeres elásticos
- Escalado de clústeres elásticos
- Fiabilidad de los clústeres elásticos
- Almacenamiento y disponibilidad de clústeres elásticos
- Diferencias funcionales entre Amazon DocumentDB 4.0 y los clústeres elásticos

Partición en los clústeres elásticos de Amazon DocumentDB

Los clústeres elásticos de Amazon DocumentDB utilizan particiones basadas en hash para hacer particiones de datos en un sistema de almacenamiento distribuido. La partición, también conocida como particionamiento, divide los conjuntos de datos grandes en conjuntos de datos pequeños en varios nodos, lo que le permite escalar la base de datos más allá de los límites de escalado vertical. Los clústeres elásticos utilizan la separación (o «disociación») del procesamiento y el

almacenamiento en Amazon DocumentDB, lo que le permite a usted escalar de forma independiente. En lugar de volver a particionar las colecciones moviendo pequeñas particiones de datos entre los nodos de cómputo, los clústeres elásticos copian los datos de manera eficiente dentro del sistema de almacenamiento distribuido.



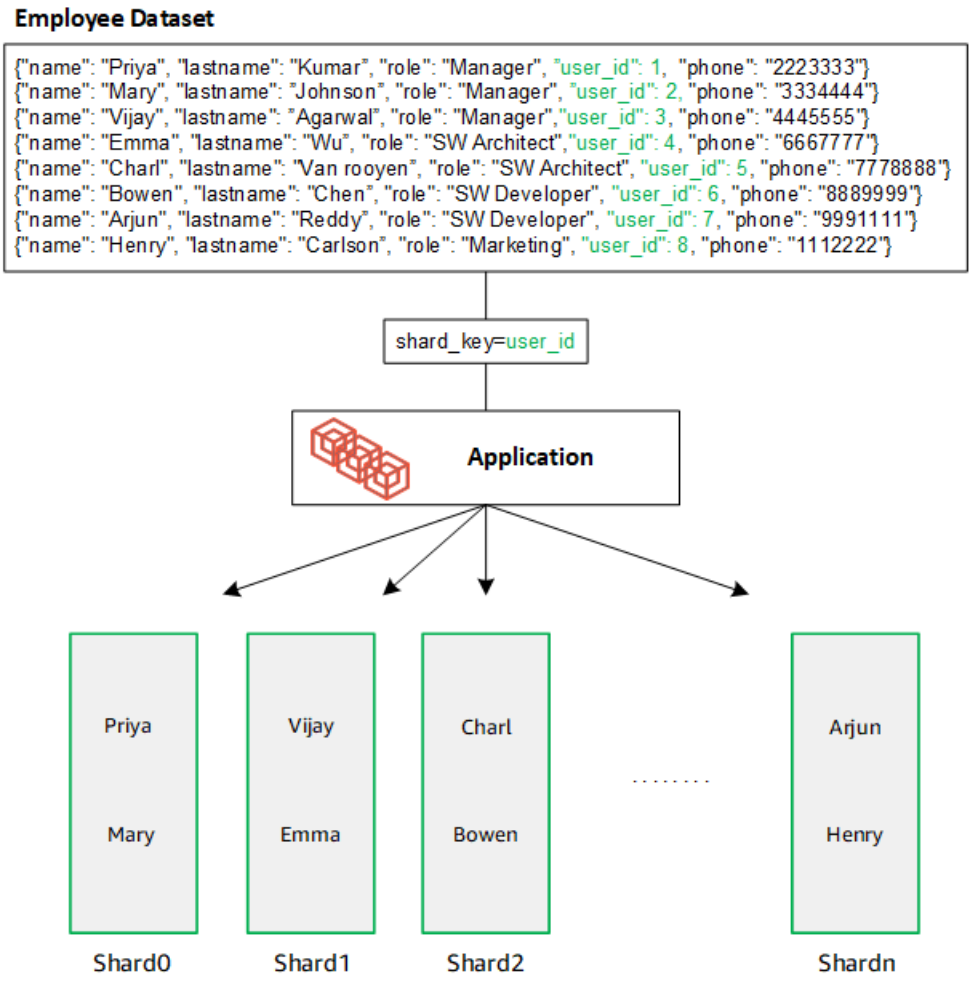
Definiciones de particiones

Definiciones de la nomenclatura de particiones:

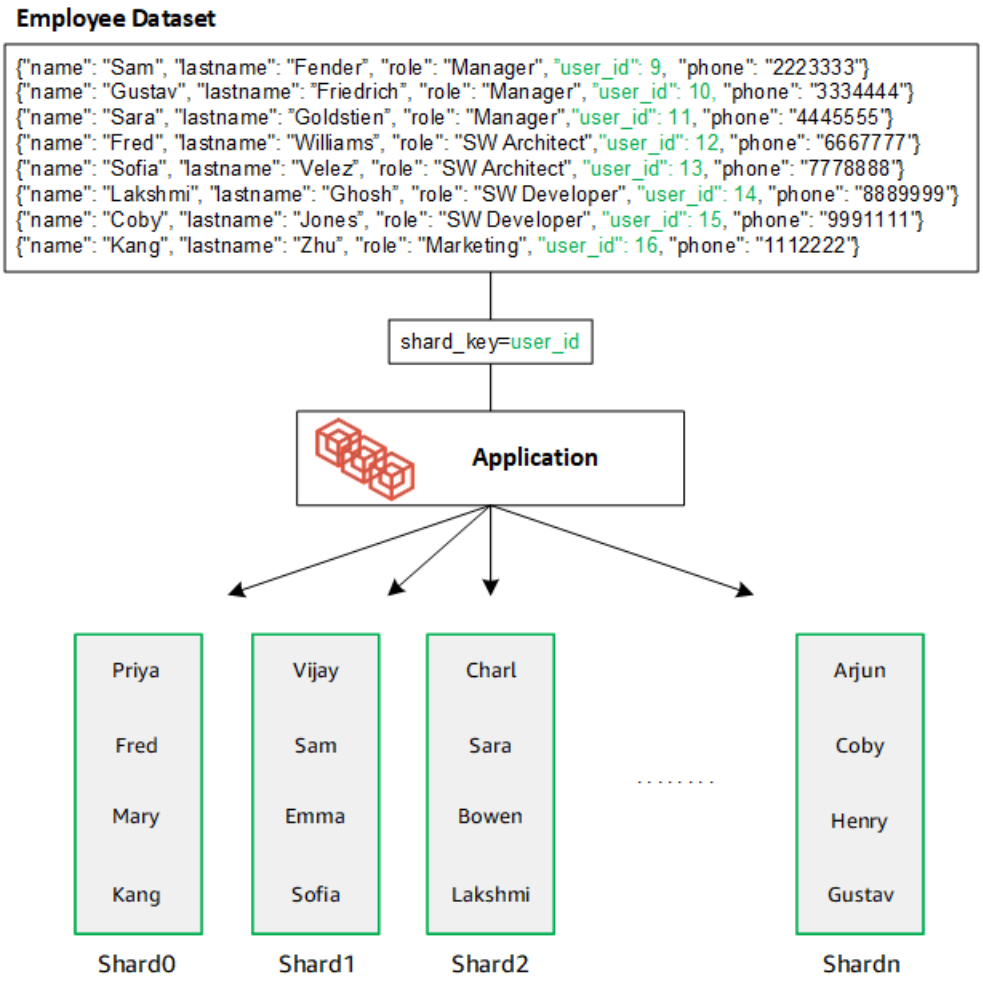
- Partición: una partición proporciona el cómputo para un clúster elástico. Tendrá una sola instancia de escritura y de 0 a 15 réplicas de lectura. De forma predeterminada, una partición tendrá dos instancias: una de escritura y una réplica de lectura única. Puede configurar un máximo de 32 particiones y cada instancia de partición puede tener un máximo de 64 v. CPUs
- Clave de partición: una clave de partición es un campo obligatorio en los documentos JSON de las colecciones con particiones, que los clústeres elásticos utilizan para distribuir el tráfico de lectura y escritura a la partición correspondiente.
- Colección con particiones: en una colección con particiones, los datos se distribuyen dentro de un clúster elástico en particiones de datos.
- Partición: una partición es una parte lógica de los datos fragmentados. Al crear una colección con particiones, los datos se organizan automáticamente en particiones dentro de cada partición en función de la clave de la partición. Cada fragmento tiene varias particiones.

Distribución de los datos entre las particiones configuradas

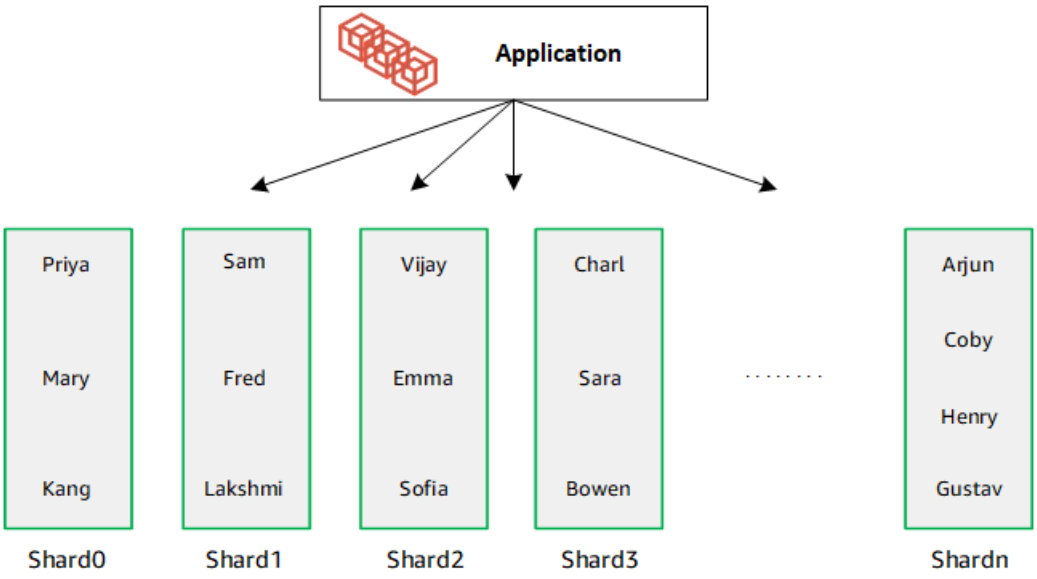
Cree una clave de partición que tenga muchos valores únicos. Una buena clave de partición particionará uniformemente sus datos entre las particiones subyacentes, proporcionando a su carga de trabajo el mejor rendimiento y desempeño. En el siguiente ejemplo, se muestran los datos del nombre de un empleado que utilizan una clave de partición denominada “user_id”:



DocumentDB utiliza la partición hash para particionar los datos en las particiones subyacentes. Los datos adicionales se insertan y distribuyen de la misma manera:



Cuando amplía la base de datos añadiendo particiones adicionales, Amazon DocumentDB redistribuye automáticamente los datos:



Migración de clústeres elásticos

Amazon DocumentDB admite la migración de datos con particiones de MongoDB a clústeres elásticos. Se admiten métodos de migración sin conexión, en línea e híbridos. Para obtener más información, consulte Migración a Amazon DocumentDB.

Escalado de clústeres elásticos

Los clústeres elásticos de Amazon DocumentDB permiten aumentar el número de fragmentos (escalado horizontal) del clúster elástico y el número de v CPUs aplicado a cada fragmento (escalado ascendente). También puede reducir la cantidad de fragmentos y la capacidad de cómputo (vCPUs) según sea necesario.

Para conocer las prácticas recomendadas de escalado, consulte Escalado de clústeres elásticos.

> **Note**
>
> También está disponible el escalado a nivel de clúster. Para obtener más información, consulte Escalado de clústeres de Amazon DocumentDB.

Fiabilidad de los clústeres elásticos

Amazon DocumentDB está diseñado para ofrecer fiabilidad, durabilidad y tolerancia a errores. Para mejorar la disponibilidad, los clústeres elásticos implementan dos nodos por partición ubicados en diferentes zonas de disponibilidad. Amazon DocumentDB también incluye varias características automáticas que la convierten en una solución de base de datos de confianza. Para obtener más información, consulte Fiabilidad de Amazon DocumentDB.

Almacenamiento y disponibilidad de clústeres elásticos

Los datos de Amazon DocumentDB se almacenan en un volumen de clúster, que es un volumen virtual único que utiliza unidades de estado sólido ()SSDs. Un volumen de clúster consta de seis copias de sus datos, que se replican automáticamente en varias zonas de disponibilidad de una sola AWS región. Esta replicación ayuda a garantizar que los datos se conserven durante mucho tiempo, con menos riesgo de que se pierdan los datos. También ayuda a garantizar que el clúster esté más disponible durante una conmutación por error, porque ya existen copias de sus datos en otras zonas de disponibilidad. Para obtener más información sobre el almacenamiento, la alta disponibilidad y la replicación, consulte Funcionamiento de Amazon DocumentDB.

Diferencias funcionales entre Amazon DocumentDB 4.0 y los clústeres elásticos

Existen las siguientes diferencias funcionales entre Amazon DocumentDB 4.0 y los clústeres elásticos.

- El resultado de `top` y `collStats` se fragmenta en particiones. En el caso de las colecciones con particiones, los datos se distribuyen entre varias particiones y a los informes de `collStats` se agrega `collScans` desde las particiones.
- Las estadísticas de recopilación de `top` y `collStats` para las colecciones con particiones se restablecen cuando se cambia el recuento de particiones del clúster.
- La función de copia de seguridad integrada ahora es compatible con `serverStatus`. Acción: los desarrolladores y las aplicaciones con función de backup pueden recopilar estadísticas sobre el estado del clúster de Amazon DocumentDB.
- El campo `SecondaryDelaySecs` reemplaza a `slaveDelay` en la salida `replSetGetConfig`.
- El comando `hello` reemplaza a `isMaster`. `hello` devuelve un documento que describe la función del clúster elástico.
- El `$elemMatch` operador de los clústeres elásticos solo hace coincidir los documentos del primer nivel de anidación de una matriz. En Amazon DocumentDB 4.0, el operador recorre todos los niveles antes de devolver los documentos coincidentes. Por ejemplo:

```
db.foo.insert(
[
    {a: {b: 5}},
    {a: {b: [5]}},
    {a: {b: [3, 7]}},
    {a: [{b: 5}]},
    {a: [{b: 3}, {b: 7}]},
    {a: [{b: [5]}]},
    {a: [{b: [3, 7]}]},
    {a: [[{b: 5}]]},
    {a: [[{b: 3}, {b: 7}]]},
    {a: [[{b: [5]}]]},
    {a: [[{b: [3, 7]}]]}
]);
// Elastic clusters
```

```
> db.foo.find({a: {$elemMatch: {b: {$elemMatch: {$lt: 6, $gt: 4}}}}}, {_id: 0})
{ "a" : [ { "b" : [ 5 ] } ] }

// Docdb 4.0: traverse more than one level deep
> db.foo.find({a: {$elemMatch: {b: {$elemMatch: {$lt: 6, $gt: 4}}}}}, {_id: 0})
{ "a" : [ { "b" : [ 5 ] } ] }
{ "a" : [ [ { "b" : [ 5 ] } ] ] }
```

- La proyección “$” de Amazon DocumentDB 4.0 devuelve todos los documentos con todos los campos. Con los clústeres elásticos, el comando `find` con una proyección “$” devuelve los documentos que coinciden con el parámetro de consulta y contienen solo el campo que coincide con la proyección “$”.
- En los clústeres elásticos, los comandos `find` con parámetros de consulta `$regex` y `$options` devuelven un error: «No se pueden establecer opciones tanto en $regex como en $options».

- Con los clústeres elásticos, `$indexOfCP` ahora devuelve “-1” cuando:
  - la subcadena no se encuentra en `string expression`, o
  - `start` es un número mayor que `end`, o
  - `start` es un número mayor que la longitud en bytes de la cadena.

  En Amazon DocumentDB 4.0, `$indexOfCP` devuelve “0” cuando la posición `start` es un número mayor que `end` o que la longitud en bytes de la cadena.
- Con los clústeres elásticos, las operaciones de proyección en `_id fields`, por ejemplo, `{"_id.nestedField" : 1}`, devuelven documentos que solo incluyen el campo proyectado. Mientras tanto, en Amazon DocumentDB 4.0, los comandos de proyección de campos anidados no filtran ningún documento.

Introducción a los clústeres elásticos de Amazon DocumentDB

En esta sección de introducción se explica cómo crear y consultar su primer clúster elástico.

Existen muchas formas de conectarse a Amazon DocumentDB y empezar a usarlo. El siguiente procedimiento es la forma más rápida, sencilla y fácil de que los usuarios comiencen a utilizar nuestra potente base de datos de documentos. En esta guía se utiliza el AWS CloudShell para conectarse al clúster de Amazon DocumentDB directamente desde la Consola de administración de AWS y consultarlo. Los nuevos clientes que reúnan los requisitos para el nivel gratuito de AWS

pueden utilizar Amazon DocumentDB y CloudShell gratis. Si su entorno de AWS CloudShell o clúster de Amazon DocumentDB hace uso de recursos más allá del nivel gratuito, se le cobrarán las tarifas de AWS normales de dichos recursos. Esta guía le permitirá empezar a utilizar Amazon DocumentDB en menos de 5 minutos.

Temas

- Requisitos previos
- Paso 1: crear un clúster elástico
- Paso 2: conectarse a su clúster elástico
- Paso 3: hacer una partición de su colección; insertar y consultar los datos
- Paso 4: explorar

Requisitos previos

Antes de crear el primer clúster de Amazon DocumentDB, debe hacer lo siguiente:

Creación de una cuenta de Amazon Web Services (AWS)

Para empezar a utilizar Amazon DocumentDB, debe tener una cuenta de Amazon Web Services (AWS). La cuenta de AWS es gratuita. Solo se paga por los servicios y los recursos que se utilicen.

Si no dispone de una Cuenta de AWS, siga estos pasos para crear una.

Procedimiento para registrarse en Cuenta de AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga las instrucciones que se le indiquen.

   Parte del procedimiento de registro consiste en recibir una llamada telefónica o mensaje de texto e indicar un código de verificación en el teclado del teléfono.

   Al registrarse en una Cuenta de AWS, se crea un Usuario raíz de la cuenta de AWS. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario y utilice únicamente el usuario raíz para realizar tareas que requieren acceso de usuario raíz.

Configure los permisos de AWS Identity and Access Management (IAM) necesarios.

El acceso para administrar los recursos de Amazon DocumentDB como clústeres, instancias y grupos de parámetros de clúster requiere credenciales que AWS puede utilizar para autenticar las solicitudes. Para obtener más información, consulte Identity and Access Management para Amazon DocumentDB.

1. En la barra de búsqueda de la Consola de administración de AWS, escriba IAM y seleccione IAM en el menú desplegable.
2. Cuando esté en la consola de IAM, seleccione Usuarios en el panel de navegación.
3. Seleccione su nombre de usuario.
4. Haga clic en Add Permission (Agregar permiso).
5. Seleccione Adjuntar políticas directamente.
6. Escriba `AmazonDocDBElasticFullAccess` en la barra de búsqueda y selecciónelo en cuanto aparezca en los resultados de búsqueda.
7. Haga clic en Next (Siguiente).
8. Haga clic en Add Permission (Agregar permiso).

> **Note**
>
> La cuenta de AWS contiene una VPC predeterminada en cada región. Si decide utilizar una Amazon VPC, complete los pasos del tema Creación de una Amazon VPC en la Guía del usuario de Amazon VPC.

Paso 1: crear un clúster elástico

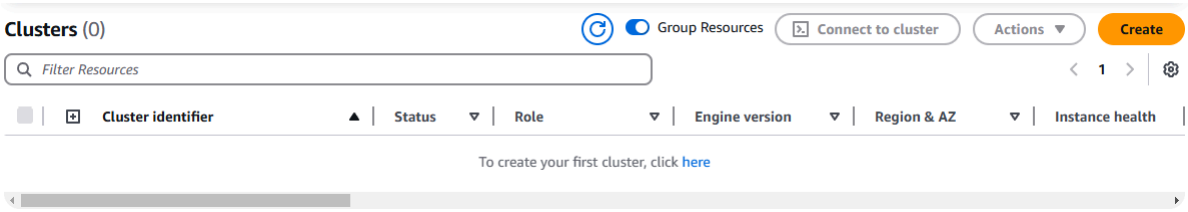
En esta sección explicamos cómo crear un clúster elástico completamente nuevo, utilizando las instrucciones siguientes en la Consola de administración de AWS o la AWS CLI.

Using the Consola de administración de AWS

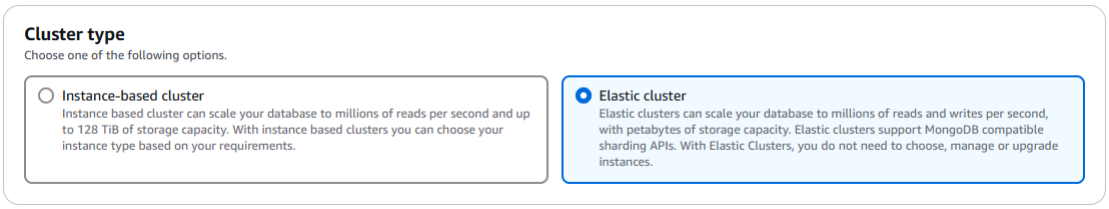
Para crear una configuración de clúster elástico mediante la Consola de administración de AWS:

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon DocumentDB en https://console.aws.amazon.com/docdb.

2. En la consola de administración de Amazon DocumentDB, en Clústeres, elija Crear.



3. En la página Crear clúster de Amazon DocumentDB, en la sección Tipo de clúster, elija clúster elástico.



4. En la sección Configuración, configure lo siguiente:

   a. En el campo Nombre del clúster, introduzca un identificador de clúster único (siguiendo los requisitos de denominación que aparecen debajo del campo).

   b. En el campo Recuento de particiones, introduzca el número de particiones que desea tener en el clúster. El número máximo de particiones por clúster es 32.

   > **Note**
   >
   > Se implementarán dos nodos para cada partición. Ambos nodos tendrán la misma capacidad de partición.

   c. En el campo Recuento de instancias de partición, elija el número de instancias de réplica que desee asociar a cada partición. El número máximo de instancias de partición es 16, en incrementos de 1. Todas las instancias de réplica tienen la misma capacidad de partición que se define en el campo siguiente. Para fines de prueba, el valor predeterminado de 2 debería ser suficiente.

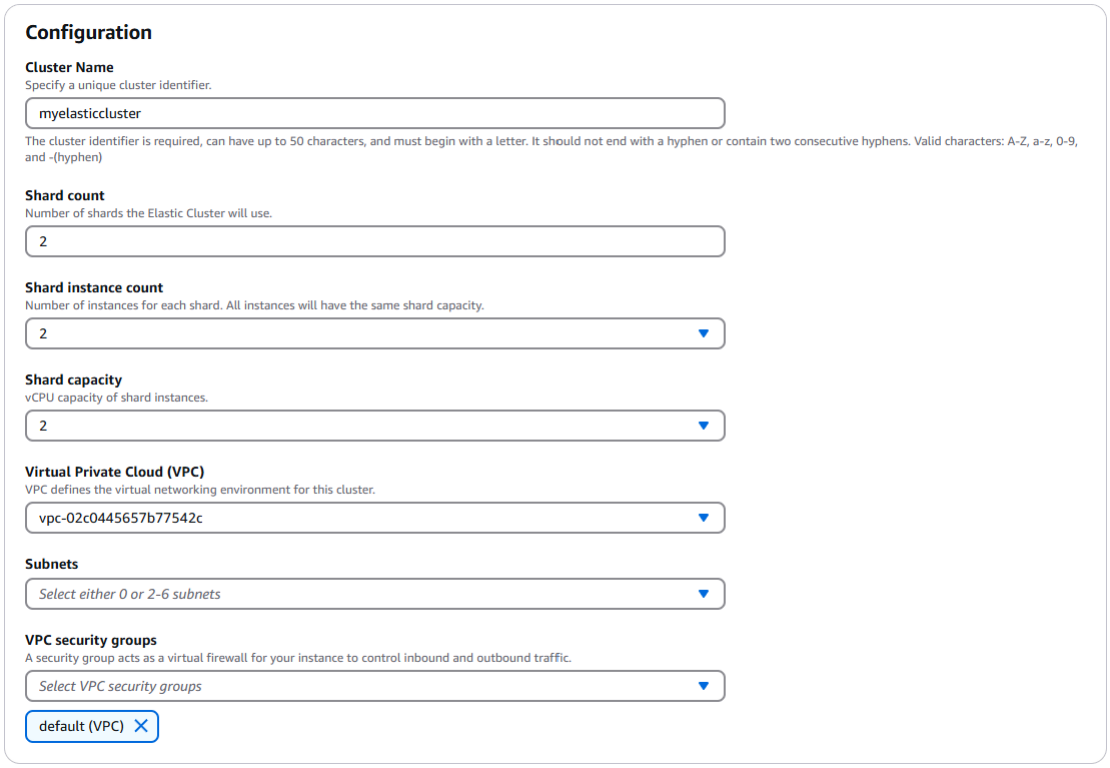
   > **Note**
   >
   > El número de instancias de réplica se aplica a todas las particiones del clúster elástico. Un valor de recuento de instancias de particiones igual a 1 significa que hay una instancia de escritura y las instancias adicionales son réplicas que se

pueden usar para llevar a cabo lecturas y mejorar la disponibilidad. Para fines de prueba, el valor predeterminado de 2 debería ser suficiente.

d. En el campo Capacidad de la partición, elija el número de CPU virtuales (vCPU) que desee asociar a cada instancia de partición. La cantidad máxima de vCPU por instancia de partición es 64. Los valores permitidos son 2, 4, 8, 16, 32, 64. Para fines de prueba, el valor predeterminado de 2 debería ser suficiente.

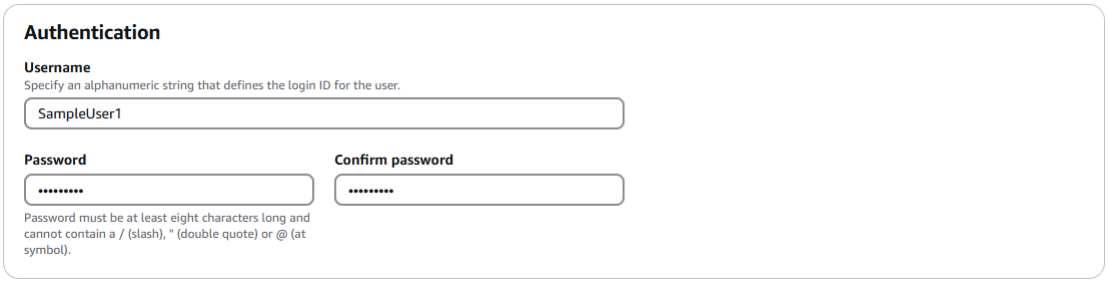
e. En el campo Nube privada virtual (VPC), elija una VPC de la lista desplegable.

f. Para las subredes y los grupos de seguridad de VPC, puede usar los valores predeterminados o seleccionar tres subredes de su elección y hasta tres grupos de seguridad de VPC (uno como mínimo).



5. En la sección Autenticación, ingrese una cadena que identifique el nombre de inicio de sesión del usuario principal en el campo Nombre de usuario.

   En el campo Contraseña, introduzca una contraseña única que cumpla con las instrucciones y, a continuación, confírmela.



6. En la sección Cifrado, mantenga la configuración predeterminada (Clave predeterminada).

   Si lo desea, puede introducir un AWS KMS key ARN que haya creado. Para obtener más información, consulte Activación del cifrado de datos en reposo de un clúster elástico de Amazon DocumentDB.

   > **Important**
   >
   > El cifrado debe estar habilitado para los clústeres elásticos.

7. En la sección Copia de seguridad, edite los campos de acuerdo con los requisitos de copia de seguridad. Para fines de prueba, puede retener la configuración predeterminada.



   a. Periodo de retención de copias de seguridad: en la lista, elija el número de días que se deben conservar las copias de seguridad automáticas de este clúster antes de eliminarlas.

   b. Periodo de copia de seguridad: especifique la hora del día en que Amazon DocumentDB debe hacer las copias de seguridad de este clúster y la duración de las mismas.

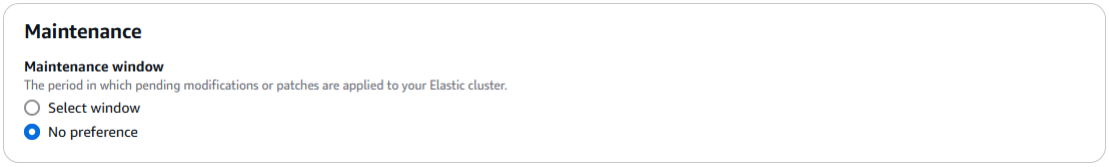
      i. Elija Seleccionar periodo si desea configurar la hora y la duración de la creación de las copias de seguridad.

         Hora de inicio: en la primera lista, elija la hora de inicio (UTC) para las copias de seguridad automáticas. En la segunda lista, elija el minuto de la hora en que desea que comiencen las copias de seguridad automáticas.

Duración: en la lista, elija el número de horas que se deben asignar para crear las copias de seguridad automáticas.

ii. Seleccione Sin preferencia si desea que Amazon DocumentDB elija la hora y la duración de la creación de las copias de seguridad.

8. En la sección Mantenimiento, elija el día, la hora y la duración en que se aplicarán las modificaciones o los parches al clúster. Para fines de prueba, puede retener la configuración predeterminada.



9. Elija Create cluster.

El clúster elástico se está aprovisionando ahora. Esto puede tardar unos minutos en terminar. Puede conectarse a su clúster cuando el estado del clúster elástico aparezca como Disponible en la lista de Clústeres.

Using the AWS CLI

Para crear un clúster elástico con la AWS CLI, utilice la operación `create-cluster` con los siguientes parámetros:

- --cluster-name: obligatorio. El nombre actual del clúster de escala elástica tal como se ingresó durante la creación o se modificó por última vez.
- --shard-capacity: obligatorio. El número de vCPU asignado a cada partición. El máximo es 64. Los valores permitidos son 2, 4, 8, 16, 32, 64.
- --shard-count: obligatorio. La cantidad de particiones asignadas al clúster. El máximo es 32.
- --shard-instance-count: opcional. El número de instancias de réplica que se aplican a todos los fragmentos de este clúster. El máximo es 16.
- --admin-user-name: obligatorio. Nombre del usuario asociado al usuario administrador.
- --admin-user-password: obligatorio. La contraseña asociada al usuario administrador.
- --auth-type: obligatorio. El tipo de autenticación utilizado para determinar dónde buscar la contraseña que se usa para acceder al clúster elástico. Los tipos válidos son `PLAIN_TEXT` o `SECRET_ARN`.

- --vpc-security-group-ids: opcional. Configure una lista de grupos de seguridad para asociar a este clúster.
- --preferred-maintenance-window: opcional. Configure el tiempo semanal durante el cual puede llevarse a cabo el mantenimiento del sistema, en tiempo universal coordinado (UTC).

  El formato es: `ddd:hh24:mi-ddd:hh24:mi`. Días válidos: lunes, martes, miércoles, jueves, viernes, sábado, domingo

  El valor predeterminado es un periodo de 30 minutos seleccionado al azar de un bloque de 8 horas de tiempo para cada región de Amazon Web Services, que tiene lugar un día de la semana de forma aleatoria.

  El plazo mínimo es 30 minutos.
- --kms-key-id: opcional. Configure el identificador de la clave de KMS de un clúster cifrado.

  El identificador de la clave de KMS es el nombre de recurso de Amazon (ARN) de la clave de cifrado de AWS KMS. Si está creando un clúster con la misma cuenta de Amazon Web Services a la que pertenece la clave de cifrado de KMS utilizada para cifrar el clúster nuevo, puede utilizar el alias de la clave de KMS en lugar del ARN para la clave de cifrado de KMS.

  Si no se especifica una clave de cifrado en KmsKeyId y si el parámetro `StorageEncrypted` es verdadero, Amazon DocumentDB utilizará su clave de cifrado predeterminada.
- --preferred-backup-window: opcional. El intervalo de tiempo diario preferido durante el que se crean las copias de seguridad automatizadas. El valor predeterminado es una ventana de 30 minutos seleccionada al azar dentro de un bloque de 8 horas para cada Región de AWS.
- --backup-retention-period: opcional. El número de días durante los que se retienen las copias de seguridad automatizadas. El valor predeterminado es 1.
- --storage-encrypted: opcional. Configura si el clúster está cifrado o no.

  `--no-storage-encrypted` especifica que el clúster no está cifrado.
- --subnet-ids: opcional. Configure los identificadores de subred de la red.

En el siguiente ejemplo, reemplace cada *`marcador de posición del usuario`* con su propia información.

> **Note**
>
> Los siguientes ejemplos incluyen la creación de una clave KMS específica. Para usar la clave KMS predeterminada, no incluya el `--kms-key-id` parámetro.

Para Linux, macOS o Unix:

```
aws docdb-elastic create-cluster \
     --cluster-name sample-cluster-123 \
     --shard-capacity 8 \
     --shard-count 4 \
     --shard-instance-count 3 \
     --auth-type PLAIN_TEXT \
     --admin-user-name testadmin \
     --admin-user-password testPassword \
     --vpc-security-group-ids ec-65f40350 \
     --kms-key-id arn:aws:docdb-elastic:us-east-1:477568257630:cluster/
b9f1d489-6c3e-4764-bb42-da62ceb7bda2 \
     --subnet-ids subnet-9253c6a3, subnet-9f1b5af9 \
     --preferred-backup-window 18:00-18:30 \
     --backup-retention-period 7
```

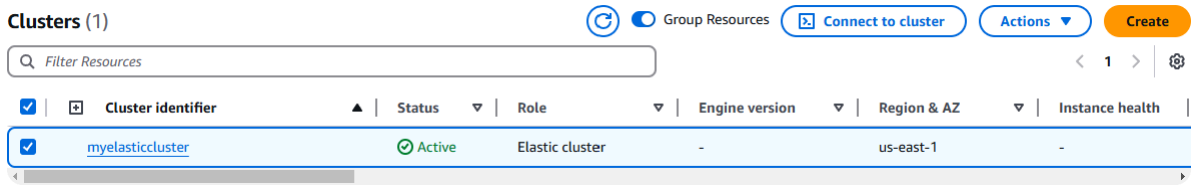
Para Windows:

```
aws docdb-elastic create-cluster ^
     --cluster-name sample-cluster-123 ^
     --shard-capacity 8 ^
     --shard-count 4 ^
     --shard-instance-count 3 ^
     --auth-type PLAIN_TEXT ^
     --admin-user-name testadmin ^
     --admin-user-password testPassword ^
     --vpc-security-group-ids ec-65f40350 ^
     --kms-key-id arn:aws:docdb-elastic:us-east-1:477568257630:cluster/
b9f1d489-6c3e-4764-bb42-da62ceb7bda2 ^
     --subnet-ids subnet-9253c6a3, subnet-9f1b5af9 \
     --preferred-backup-window 18:00-18:30 \
     --backup-retention-period 7
```

Paso 2: conectarse a su clúster elástico

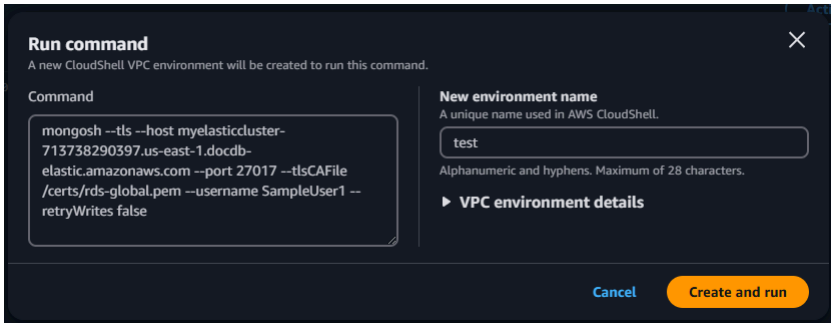
Conéctese al clúster elástico de Amazon DocumentDB con AWS CloudShell.

1. En la consola de administración de Amazon DocumentDB, en Clústeres, localice el clúster elástico que ha creado. Para elegir el clúster, haga clic en la casilla de verificación situada junto a él.



2. Haga clic en Conectarse al clúster (que se encuentra junto al menú desplegable Acciones). Este botón se activa solamente después de haber hecho clic en la casilla de verificación situada junto al clúster y el estado del clúster se muestra como Disponible. Aparece la pantalla Ejecutar comando de CloudShell.

3. En el campo Nombre del nuevo entorno, ingrese un nombre único, como «prueba» y elija Crear y ejecutar. Los detalles del entorno de la VPC se configuran automáticamente para la base de datos de Amazon DocumentDB.



4. Cuando vea la petición, introduzca la contraseña que creó en el Paso 1: crear un clúster elástico de Amazon DocumentDB (subpaso 5).



Después de ingresar la contraseña y de que la petición se convierte en `direct: mongos] <env-name>>`, significa que se ha conectado correctamente al clúster de Amazon DocumentDB.

> **Note**
>
> Para obtener información sobre la solución de problemas, consulte Solución de problemas de Amazon DocumentDB.

Paso 3: hacer una partición de su colección; insertar y consultar los datos

Los clústeres elásticos aportan compatibilidad para crear particiones en Amazon DocumentDB. Ahora que está conectado a su clúster, puede hacer particiones, insertar datos y ejecutar algunas consultas.

1. Para hacer particiones en una colección, escriba lo siguiente:

```
sh.shardCollection("db.Employee1" , { "Employeeid" : "hashed" })
```

2. Para insertar un solo documento, escriba lo siguiente:

```
db.Employee1.insertOne({"Employeeid":1, "Name":"Joe", "LastName": "Bruin", "level":
 1 })
```

   Se muestra lo siguiente:

```
WriteResult({ "nInserted" : 1 })
```

3. Para leer el documento que escribió, introduzca el comando `findOne()` (devuelve un único documento):

```
db.Employee1.findOne()
```

   Se muestra lo siguiente:

```
{
"_id" : ObjectId("61f344e0594fe1a1685a8151"),
```

```
"EmployeeID" : 1,
"Name" : "Joe",
"LastName" : "Bruin",
"level" : 1
}
```

4. Para realizar algunas consultas más, plantéese un caso de uso de perfil de juegos. Primero, inserte algunas entradas en una colección titulada “Empleado”. Introduzca lo siguiente:

```
db.profiles.insertMany([ { "_id": 1, "name": "Matt", "status": "active", "level":
 12, "score": 202 },
    { "_id": 2, "name": "Frank", "status": "inactive", "level": 2, "score": 9 },
    { "_id": 3, "name": "Karen", "status": "active", "level": 7, "score": 87 },
    { "_id": 4, "name": "Katie", "status": "active", "level": 3, "score": 27 }
])
```

Se muestra lo siguiente:

```
{ acknowledged: true,
     insertedIds: {
        '0': ObjectId('679d02cd6b5a0581be78bcbd'),
        '1': ObjectId('679d02cd6b5a0581be78bcbe'),
        '2': ObjectId('679d02cd6b5a0581be78bcbf'),
        '3': ObjectId('679d02cd6b5a0581be78bcc0')
    }
}
```

5. Para devolver todos los documentos de la colección de perfiles, introduzca el comando `find` ():

```
db.Employee.find()
```

Se muestran los datos que ingresó en el paso 4.

6. Para consultar un solo documento, incluya un filtro (por ejemplo: “Katie”). Introduzca lo siguiente:

```
db.Employee.find({name: "Katie"})
```

Se muestra lo siguiente:

```
[
```

```
   {

     _id: ObjectId('679d02cd6b5a0581be78bcc0'),

     Employeeid: 4,

     name: 'Katie',

     lastname: 'Schaper',

     level: 3

   }

]
```

7. Para buscar un perfil y modificarlo, introduzca el comando `findAndModify`. En este ejemplo, al empleado “Matt” se le asigna un nivel superior de “14”:

```
db.Employee.findAndModify({
    query: { "Employeeid" : 1, "name" : "Matt"},
    update: { "Employeeid" : 1, "name" : "Matt", "lastname" : "Winkle", "level" :
 14 }
})
```

   Aparece el siguiente resultado (tenga en cuenta que el nivel no ha cambiado todavía):

```
{

   _id: ObjectId('679d02cd6b5a0581be78bcbd'),

   Employeeid: 1,

   name: 'Matt',

   lastname: 'Winkle',

   level: 12

}
```

8. Para verificar el aumento de nivel, introduzca la siguiente consulte:

```
db.Employee.find({name: "Matt"})
```

Se muestra lo siguiente:

```
[
   {

   _id: ObjectId('679d02cd6b5a0581be78bcbd'),

   Employeeid: 1,

   name: 'Matt',

   lastname: 'Winkle',

   level: 14

   }
]
```

Paso 4: explorar

¡Enhorabuena! Ha completado correctamente el procedimiento de introducción a los clústeres elásticos de Amazon DocumentDB.

Pasos siguientes Descubra cómo aprovechar al máximo esta base de datos con algunas de sus características más populares:

- Prácticas recomendadas para los clústeres elásticos de Amazon DocumentDB
- Administración de los clústeres elásticos de Amazon DocumentDB

> **Note**
>
> El clúster elástico que creó a partir de este procedimiento de introducción seguirá acumulando costos a menos que lo elimine. Para obtener instrucciones, consulte Eliminación de un clúster elástico.

Prácticas recomendadas para los clústeres elásticos de Amazon DocumentDB

Descubra las mejores prácticas para trabajar con clústeres elásticos de Amazon DocumentDB. Todas las mejores recomendadas para los clústeres de Amazon DocumentDB basados en instancias también se aplican a los clústeres elásticos. Esta sección se actualiza continuamente a medida que se identifican nuevas prácticas recomendadas.

Temas

- Elección de las claves de partición
- Administración de conexiones
- Colecciones sin particiones
- Escalado de clústeres elásticos
- Monitoreo de clústeres elásticos

Elección de las claves de partición

En la siguiente lista se describen las pautas para crear claves de partición.

- Utilice una clave hash distribuida uniformemente para distribuir los datos en todos las particiones del clúster (evite las teclas de acceso rápido).
- Use su clave de partición en todas las solicitudes de lectura, actualización o eliminación para evitar consultas dispersas y agrupadas.
- Evite las claves de partición anidadas al realizar operaciones de lectura, actualización o eliminación.
- Al realizar operaciones por lotes, establezca `ordered` en falso para que todos las particiones puedan ejecutarse en paralelo y mejorar las latencias.

Administración de conexiones

En la siguiente lista se describen las pautas para administrar las conexiones con la base de datos.

- Supervise el número de conexiones y la frecuencia con la que se abren y cierran nuevas conexiones.

- Distribuya sus conexiones en todas las subredes de la configuración de su aplicación. Si su clúster está configurado en varias subredes, pero solo utiliza un subconjunto de las subredes, es posible que el número máximo de conexiones sea limitado.

Colecciones sin particiones

A continuación, se describe una guía para las colecciones sin particiones.

- Cuando trabaje con colecciones sin particiones, al distribuir la carga intente mantener las colecciones sin particiones que se usen mucho, en diferentes bases de datos. Los clústeres elásticos de Amazon DocumentDB colocan las bases de datos en diferentes particiones y comparten la ubicación de colecciones sin particiones de la misma base de datos en la misma partición.

Escalado de clústeres elásticos

En la siguiente lista se describen las pautas para escalar los clústeres elásticos.

- Las operaciones de escalado pueden provocar un breve período de errores intermitentes en la base de datos y en la red. Siempre que sea posible, evite escalar durante las horas pico. Intente escalar durante los periodos de mantenimiento.
- Es preferible aumentar y reducir la capacidad de las particiones (cambiar el recuento de vCPU por partición) para aumentar el cómputo en lugar de aumentar o disminuir el recuento de particiones, ya que es más rápido y tiene una duración más corta de los errores intermitentes de la base de datos y de la red.
- Al anticipar el crecimiento, opte por aumentar el número de particiones en lugar de escalar la capacidad de las particiones. Esto le permite escalar su clúster aumentando la capacidad de las particiones en situaciones en las que necesite escalar rápidamente.
- Supervise las políticas de reintentos del cliente y vuelva a intentarlo con retrocesos exponenciales y fluctuaciones para evitar sobrecargar la base de datos cuando se produzcan errores al escalar.

Monitoreo de clústeres elásticos

En la siguiente lista se describen las pautas para monitorear los clústeres elásticos.

- Realice un seguimiento de la relación entre el pico y el promedio de sus métricas por partición para determinar si está generando un tráfico irregular (cuente con una tecla de acceso rápido o un punto de acceso rápido). Las métricas clave para hacer un seguimiento de las proporciones entre picos y promedios son las siguientes:
  - `PrimaryInstanceCPUUtilization`
    - Esto se puede monitorear a nivel de cada partición.
    - A nivel de clúster, puede monitorear la desviación media de p99.
  - `PrimaryInstanceFreeableMemory`
    - Esto se puede monitorear a nivel de cada partición.
    - A nivel de clúster, puede monitorear la desviación media de p99.
  - `DatabaseCursorsMax`
    - Esto se debe supervisar a nivel de partición para determinar el sesgo.
  - `Documents-Inserted/Updated/Returned/Deleted`
    - Esto se debe supervisar a nivel de partición para determinar el sesgo.

Administración de los clústeres elásticos de Amazon DocumentDB

Para administrar un clúster de Amazon DocumentDB, debe disponer de una política de IAM con los permisos del plano de control de Amazon DocumentDB. Estos permisos le permiten crear, modificar y eliminar clústeres. La política de DBFull acceso a documentos de Amazon proporciona todos los permisos necesarios para administrar un clúster elástico de Amazon DocumentDB.

En los temas siguientes se muestra cómo realizar diversas tareas al trabajar con clústeres elásticos de Amazon DocumentDB.

Temas

- Modificación de configuraciones de clústeres elásticos
- Monitoreo de un clúster elástico
- Eliminación de un clúster elástico
- Administración de instantáneas de los clústeres elásticos
- Detención e inicio de un clúster elástico de Amazon DocumentDB
- Mantenimiento de clústeres elásticos de Amazon DocumentDB

Modificación de configuraciones de clústeres elásticos

En esta sección, explicamos cómo modificar el clúster elástico mediante las instrucciones siguientes Consola de administración de AWS o AWS CLI siguiendo estas instrucciones.

Un uso principal de la modificación del clúster es escalar los fragmentos aumentando o disminuyendo la capacidad de and/or cómputo de los fragmentos.

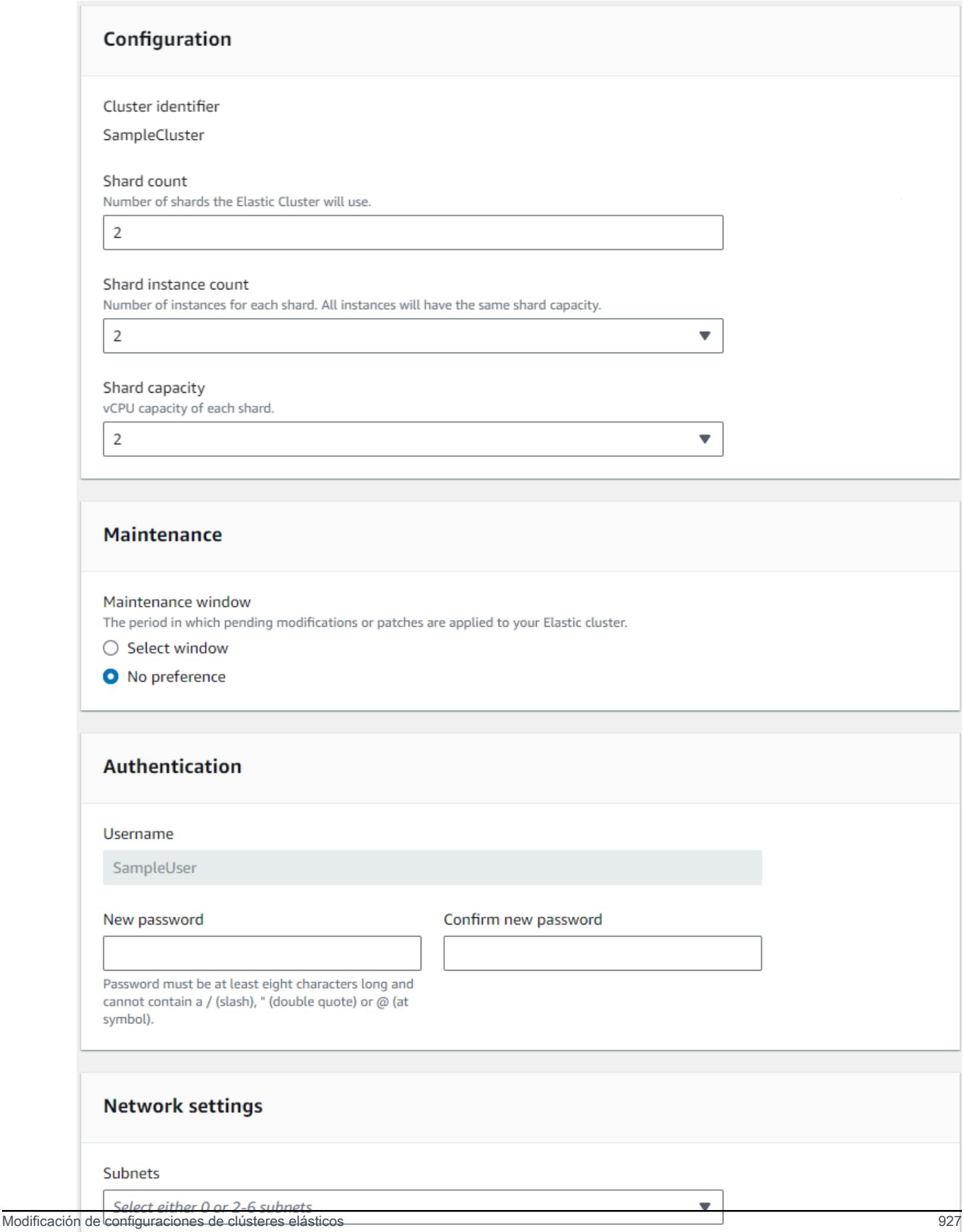
Using the Consola de administración de AWS

Para modificar la configuración de un clúster elástico mediante: Consola de administración de AWS

1. Inicie sesión en la Consola de administración de AWS de Amazon DocumentDB y ábrala.
2. En el panel de navegación, seleccione Clusters (Clústeres).

> **Tip**
>
> Si no ve el panel de navegación del lado izquierdo de la pantalla, seleccione el icono de menú en la esquina superior izquierda del panel de navegación.

3. Elija el nombre del clúster que desea modificar en la columna Identificador de clúster.
4. Elija Modificar.
5. Edite los campos que desee cambiar y, a continuación, seleccione Modificar clúster.


Configuration
Cluster identifier
SampleCluster
Shard count
Number of shards the Elastic Cluster will use.
2
Shard instance count
Number of instances for each shard. All instances will have the same shard capacity.
2
Shard capacity
vCPU capacity of each shard.
2
Maintenance
Maintenance window
The period in which pending modifications or patches are applied to your Elastic cluster.
Select window
No preference
Authentication
Username
SampleUser
New password
Confirm new password
Password must be at least eight characters long and cannot contain a / (slash), " (double quote) or @ (at symbol).
Network settings
Subnets
Select either 0 or 2-6 subnets
subnet-0b2962f92a0f5a8fb
subnet-08c6d849efd4dfe96
VPC security groups

> **Note**
>
> Como alternativa, puede acceder al cuadro de diálogo Modificar clúster desde la página Clústeres si marca la casilla situada junto al clúster, selecciona Acciones y, a continuación, Modificar.

Using the AWS CLI

Para modificar una configuración de clúster elástico mediante el AWS CLI, utilice la `update-cluster` operación con los siguientes parámetros:

- **`--cluster-arn`**: obligatorio. El identificador del ARN del clúster que desee modificar.
- **`--shard-capacity`**: opcional. El número de v CPUs asignado a cada fragmento. El máximo es 64. Los valores permitidos son 2, 4, 8, 16, 32, 64.
- **`--shard-count`**: opcional. La cantidad de particiones asignadas al clúster. El máximo es 32.
- Recuento de **`--shard-instance`**: opcional. El número de instancias de réplica que se aplican a todos los fragmentos de este clúster. El máximo es 16.
- **`--auth-type`**: opcional. El tipo de autenticación utilizado para determinar dónde buscar la contraseña que se usa para acceder al clúster elástico. Los tipos válidos son `PLAIN_TEXT` o `SECRET_ARN`.
- **`--admin-user-password`**: opcional. La contraseña asociada al usuario administrador.
- **`--vpc-security-group-ids`**: opcional. Configure una lista de grupos de seguridad de Amazon EC2 y Amazon Virtual Private Cloud (VPC) para asociarlos a este clúster.
- **`--preferred-maintenance-window`**: opcional. El intervalo de tiempo semanal durante el cual puede llevarse a cabo el mantenimiento del sistema, en tiempo universal coordinado (UTC).

  El formato es: `ddd:hh24:mi-ddd:hh24:mi`. Días válidos: lunes, martes, miércoles, jueves, viernes, sábado, domingo

  El valor predeterminado es un periodo de 30 minutos seleccionado al azar de un bloque de 8 horas de tiempo para cada región de Amazon Web Services, que tiene lugar un día de la semana de forma aleatoria.

  El plazo mínimo es 30 minutos.
- **`--subnet-ids`**: opcional. Configure los identificadores de subred de la red.

Para utilizar el ejemplo siguiente, sustituya *user input placeholder* con su propia información.

Para Linux, macOS o Unix:

```
aws docdb-elastic update-cluster \
    --cluster-arn arn:aws:docdb-elastic:us-east-1:477568257630:cluster/
b9f1d489-6c3e-4764-bb42-da62ceb7bda2 \
    --shard-capacity 8 \
    --shard-count 4 \
    --shard-instance-count 3 \
    --admin-user-password testPassword \
    --vpc-security-group-ids ec-65f40350 \
    --subnet-ids subnet-9253c6a3, subnet-9f1b5af9
```

Para Windows:

```
aws docdb-elastic update-cluster ^
    --cluster-arn arn:aws:docdb-elastic:us-east-1:477568257630:cluster/
b9f1d489-6c3e-4764-bb42-da62ceb7bda2 ^
    --shard-capacity 8 ^
    --shard-count 4 ^
    --shard-instance-count 3 ^
    --admin-user-password testPassword ^
    --vpc-security-group-ids ec-65f40350 ^
    --subnet-ids subnet-9253c6a3, subnet-9f1b5af9
```

Para supervisar el estado del clúster elástico después de la modificación, consulte Supervisión de un clúster elástico.

Monitoreo de un clúster elástico

En esta sección, explicamos cómo monitorizar el clúster elástico mediante las instrucciones siguientes Consola de administración de AWS o AWS CLI siguiendo estas instrucciones.

Using the Consola de administración de AWS

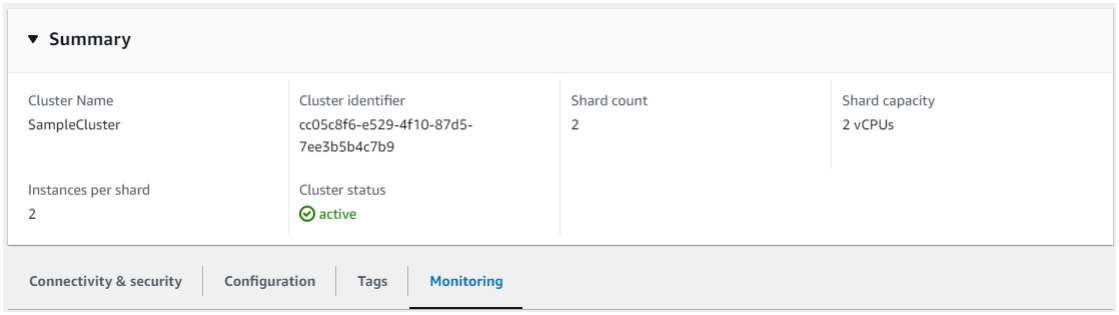
Para monitorear la configuración de un clúster elástico mediante Consola de administración de AWS:

1. Inicie sesión en la Consola de administración de AWS de Amazon DocumentDB y ábrala.

2. En el panel de navegación, seleccione Clusters (Clústeres).

> **Tip**
>
> Si no ve el panel de navegación del lado izquierdo de la pantalla, seleccione el icono de menú en la esquina superior izquierda del panel de navegación.

3. Elija el nombre del clúster que desea monitorear en la columna del Identificador del clúster.
4. Elija la pestaña Monitorización.



Se muestran varios gráficos de Amazon CloudWatch para las siguientes categorías de seguimiento:

- Uso de los recursos
- Rendimiento
- Operaciones
- Sistema

También puede acceder a Amazon CloudWatch a través de Consola de administración de AWS para configurar su propio entorno de monitoreo para sus clústeres elásticos.

Using the AWS CLI

Para monitorear una configuración de clúster elástico específica mediante el AWS CLI, utilice la `get-cluster` operación con los siguientes parámetros:

- **`--cluster-arn`**: obligatorio. Identificador del ARN del clúster para el que desea obtener información detallada.

Para utilizar el ejemplo siguiente, sustituya *`user input placeholder`* con su propia información.

Para Linux, macOS o Unix:

```
aws docdb-elastic get-cluster \
    --cluster-arn arn:aws:docdb-elastic:us-west-2:123456789012:cluster:/68ffcdf8-e3af-40a3-91e4-24736f2dacc9
```

Para Windows:

```
aws docdb-elastic get-cluster ^
    --cluster-arn arn:aws:docdb:-elastic:us-west-2:123456789012:cluster:/68ffcdf8-e3af-40a3-91e4-24736f2dacc9
```

La salida de esta operación será similar a lo que se indica a continuación:

```
"cluster": {
        ...
        "clusterArn": "arn:aws:docdb-elastic:us-
west-2:123456789012:cluster:/68ffcdf8-e3af-40a3-91e4-24736f2dacc9",
        "clusterEndpoint": "stretch-11-477568257630.us-east-1.docdb-
elastic.amazonaws.com",
        "readerEndpoint": "stretch-11-477568257630-ro.us-east-1.docdb-
elastic.amazonaws.com",
        "clusterName": "stretch-11",
        "shardCapacity": 2,
        "shardCount": 3,
        "shardInstanceCount: 5,
        "status": "ACTIVE",
        ...
 }
```

Para obtener más información, consulte `DescribeClusterSnapshot` en la Referencia de la API para administración de recursos de Amazon DocumentDB.

Para ver los detalles de todos los clústeres elásticos que utilizan el AWS CLI, utilice la `list-clusters` operación con los siguientes parámetros:

- **`--next-token`**: opcional. Si el número de elementos de salida (`--max-results`) es inferior al número total de elementos devueltos por las llamadas básicas a la API, la salida incluirá un

`NextToken` que podrá pasar a un comando posterior para recuperar el siguiente conjunto de elementos.

- **`--max-results`**: opcional. El número total de elementos que se devuelven en la salida del comando. Si el número de registros es superior al valor `max-results` especificado, se incluye en la respuesta un token de paginación (`next-token`) que se conoce como marcador, de modo que se pueda recuperar el resto de resultados.
  - Predeterminado: 100
  - Mínimo = 20, máximo = 100

Para utilizar el ejemplo siguiente, sustituya *`user input placeholder`* con su propia información.

Para Linux, macOS o Unix:

```
aws docdb-elastic list-clusters \
    --next-token eyJNYXJrZXIiOiBudWxsLCAiYm90b190cnVuY2F0ZV9hbW91bnQiOiAxfQ== \
    --max-results 2
```

Para Windows:

```
aws docdb-elastic list-clusters ^
    --next-token eyJNYXJrZXIiOiBudWxsLCAiYm90b190cnVuY2F0ZV9hbW91bnQiOiAxfQ== ^
    --max-results 2
```

La salida de esta operación será similar a lo que se indica a continuación:

```
{
   "Clusters": [
      {
         "ClusterIdentifier":"mycluster-1",
         "ClusterArn":"arn:aws:docdb:us-west-2:123456789012:sharded-cluster:sample-
cluster"
         "Status":"available",
         "ClusterEndpoint":"sample-cluster.sharded-cluster-corcjozrlsfc.us-
west-2.docdb.amazonaws.com"
       }
       {
         "ClusterIdentifier":"mycluster-2",
         "ClusterArn":"arn:aws:docdb:us-west-2:987654321098:sharded-cluster:sample-
cluster"
```

```
         "Status":"available",
         "ClusterEndpoint":"sample-cluster2.sharded-cluster-corcjozrlsfc.us-
west-2.docdb.amazonaws.com"
       }
   ]
}
```

Eliminación de un clúster elástico

En esta sección, explicamos cómo eliminar un clúster elástico, utilizando las instrucciones siguientes Consola de administración de AWS o AWS CLI siguiendo estas instrucciones.

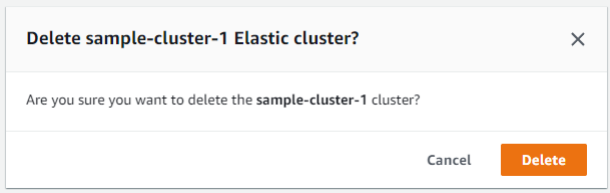
Using the Consola de administración de AWS

Para eliminar una configuración de clúster elástico mediante la Consola de administración de AWS:

1. Inicie sesión en la Consola de administración de AWS de Amazon DocumentDB y ábrala.
2. En el panel de navegación, seleccione Clusters (Clústeres).

> **Tip**
>
> Si no ve el panel de navegación del lado izquierdo de la pantalla, seleccione el icono de menú en la esquina superior izquierda del panel de navegación.

3. En la tabla de lista de clúster, active la casilla de verificación situada a la izquierda del nombre del clúster que desea eliminar y, a continuación, elija Acciones. En el menú desplegable, seleccione Eliminar.
4. ¿En el clúster elástico Eliminar “cluster-name”? cuadro de diálogo, elija Eliminar.



La eliminación del clúster puede tardar varios minutos. Para supervisar el estado del clúster, consulte Supervisión del estado de un clúster de Amazon DocumentDB.

Using the AWS CLI

Para eliminar un clúster elástico mediante AWS CLI, utilice la `delete-cluster` operación con los siguientes parámetros:

- **`--cluster-arn`**: obligatorio. El identificador del ARN del clúster que desee eliminar.
- **`--no-skip-final-backup`**: opcional. Si desea una instantánea final, debe incluir este parámetro con un nombre para la instantánea final. Debe incluir `--final-backup-identifier` o `--skip-final-backup`.
- **`--skip-final-backup`**: opcional. Use este parámetro solo si no desea realizar un respaldo final antes de eliminar el clúster. El comportamiento predeterminado es realizar una instantánea final.

Los siguientes ejemplos de AWS CLI código eliminan un clúster con un ARN de arn:aws:docdb:us-west- 2:123456789012:sharded-cluster:sample-cluster con una copia de seguridad final.

En el siguiente ejemplo, sustituya cada uno por su propia información. *`user input placeholder`*

Para Linux, macOS o Unix:

```
aws docdb-elastic delete-cluster \
    --cluster-arn arn:aws:docdb:us-west-2:123456789012:sharded-cluster:sample-cluster \
    --no-skip-final-backup \
    --final-backup-identifier finalArnBU-arn:aws:docdb:us-west-2:123456789012:sharded-cluster:sample-cluster
```

Para Windows:

```
aws docdb-elastic delete-cluster ^
    --cluster-arn arn:aws:docdb:us-west-2:123456789012:sharded-cluster:sample-cluster ^
    --no-skip-final-backup ^
    --final-backup-identifier finalArnBU-arn:aws:docdb:us-west-2:123456789012:sharded-cluster:sample-cluster
```

Los siguientes ejemplos de AWS CLI código eliminan un clúster con un ARN de arn:aws:docdb:us-west- 2:123456789012:sharded-cluster:sample-cluster sin realizar una copia de seguridad final.

Para utilizar el ejemplo siguiente, sustituya *user input placeholder* con su propia información.

Para Linux, macOS o Unix:

```
aws docdb-elastic delete-cluster \
    --cluster-arn arn:aws:docdb:us-west-2:123456789012:sharded-cluster:sample-cluster \
    --skip-final-backup \
```

Para Windows:

```
aws docdb-elastic delete-cluster ^
    --cluster-arn arn:aws:docdb:us-west-2:123456789012:sharded-cluster:sample-cluster ^
    --skip-final-backup ^
```

El resultado de la operación `delete-cluster` es el clúster que se va a eliminar.

La eliminación del clúster puede tardar varios minutos. Para supervisar el estado del clúster, consulte Supervisión del estado de un clúster de Amazon DocumentDB.

Administración de instantáneas de los clústeres elásticos

Se pueden realizar instantáneas manuales después de crear un clúster elástico. Las copias de seguridad automatizadas se crean en el momento en que se crea la instantánea del clúster elástico.

> **Note**
>
> Su clúster elástico debe estar en estado `Available` para que se tome una instantánea manual.

En esta sección se explica cómo puede crear, ver, restaurar y eliminar instantáneas de clústeres elásticos.

En los temas siguientes se muestra cómo realizar diversas tareas al trabajar con instantáneas de clústeres elásticos de Amazon DocumentDB.

Temas

- Creación de una instantánea manual del clúster
- Visualización de una instantánea de un clúster elástico
- Restauración de un clúster desde una instantánea
- Copia de una instantánea de un clúster elástico
- Eliminar una instantánea de un clúster elástico
- Administración de una copia de seguridad automática de una instantánea de un clúster elástico

Creación de una instantánea manual del clúster

En esta sección, explicamos cómo crear una instantánea manual de un clúster elástico, utilizando las instrucciones siguientes o siguiendo estas instrucciones. Consola de administración de AWS AWS CLI

Using the Consola de administración de AWS

Para crear una instantánea manual de un clúster elástico mediante la Consola de administración de AWS:

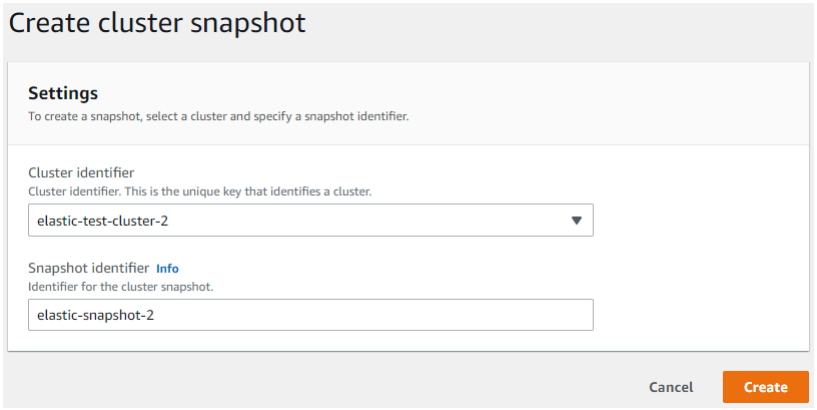
1. Inicie sesión en la Consola de administración de AWS de Amazon DocumentDB y ábrala.
2. En el panel de navegación, elija Snapshots (Instantáneas).

   > **Tip**
   >
   > Si no ve el panel de navegación del lado izquierdo de la pantalla, seleccione el icono de menú en la esquina superior izquierda del panel de navegación.

3. En la página Snapshots (Instantáneas), elija Create (Crear).
4. En la página Crear una instantánea de clúster, en el campo Identificador del clúster, elija su clúster elástico en la lista desplegable.

   En el campo Identificador de instantáneas, introduce un identificador único para tu clúster elástico.

Seleccione Crear.



> **Note**
>
> Como alternativa, puede acceder al cuadro de diálogo Crear una instantánea del clúster desde la página Clústeres, marcando la casilla situada junto al clúster, seleccionando Acciones y, a continuación, Realizar instantánea.

La instantánea de su clúster elástico se está aprovisionando. Esto puede tardar unos minutos en terminar. Puede verla y restaurarla desde su instantánea cuando el estado se muestre como `Available` en la lista de instantáneas.

Using the AWS CLI

Para crear una instantánea manual de un clúster elástico mediante AWS CLI, utilice la `create-cluster-snapshot` operación con los siguientes parámetros:

- **`--snapshot-name`**: obligatorio. El nombre de la instantánea para crear un nuevo clúster.
- **`--cluster-arn`**: obligatorio. El identificador del ARN del clúster del que desea crear una instantánea.

Para utilizar el ejemplo siguiente, sustituya *`user input placeholder`* con su propia información.

Para Linux, macOS o Unix:

```
aws docdb-elastic create-cluster-snapshot \
```

```
    --snapshot-name sample-snapshot-1 \
    --cluster-arn arn:aws:docdb:us-west-2:123456789012:sharded-cluster:sample-
cluster
```

Para Windows:

```
aws docdb-elastic create-cluster-snapshot ^
    --snapshot-name sample-snapshot-1 ^
    --cluster-arn arn:aws:docdb:us-west-2:123456789012:sharded-cluster:sample-
cluster
```

Visualización de una instantánea de un clúster elástico

En esta sección, explicamos cómo ver la información de las instantáneas del clúster elástico, utilizando las instrucciones siguientes Consola de administración de AWS o AWS CLI siguiendo estas instrucciones.

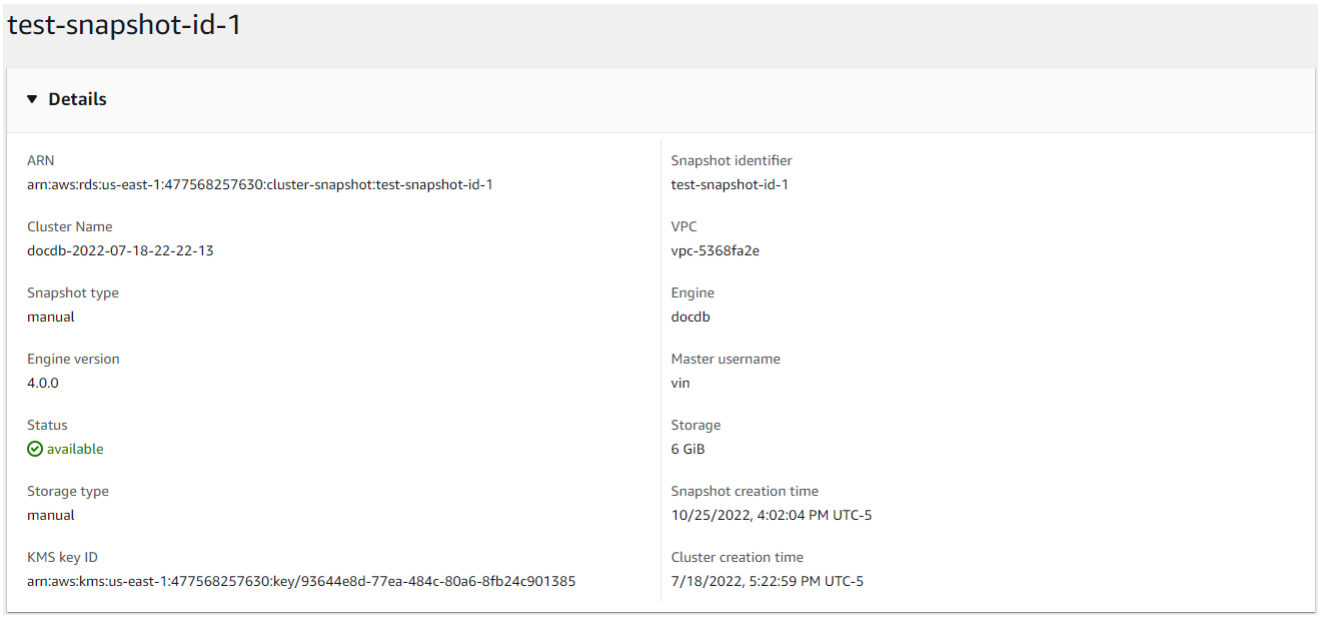
Using the Consola de administración de AWS

Para ver información sobre una instantánea específica de un clúster elástico mediante Consola de administración de AWS:

1. Inicie sesión en la Consola de administración de AWS de Amazon DocumentDB y ábrala.
2. En el panel de navegación, elija Snapshots (Instantáneas).

   > **Tip**
   >
   > Si no ve el panel de navegación del lado izquierdo de la pantalla, seleccione el icono de menú en la esquina superior izquierda del panel de navegación.

3. En la página de instantáneas, elija su instantánea de la lista haciendo clic en el nombre en la columna de identificación de instantáneas.
4. Consulta la información de la instantánea en Detalles.



Using the AWS CLI

Para ver información sobre una instantánea de un clúster elástico específica mediante el AWS CLI, utilice la `get-cluster-snapshot` operación con los siguientes parámetros:

- **`--snapshot-arn`**: obligatorio. El identificador del ARN de la instantánea de la que desea obtener información.

Para utilizar el ejemplo siguiente, sustituya *`user input placeholder`* con su propia información.

Para Linux, macOS o Unix:

```
aws docdb-elastic get-cluster-snapshot \
    --snapshot-arn sampleResourceName
```

Para Windows:

```
aws docdb-elastic get-cluster-snapshot ^
    --snapshot-arn sampleResourceName
```

Para ver información sobre una instantánea de un clúster elástico específica mediante el AWS CLI, utilice la `get-cluster-snapshot` operación con los siguientes parámetros:

- **`--snapshot-arn`**: obligatorio. El identificador del ARN de la instantánea de la que desea obtener información.

Para utilizar el ejemplo siguiente, sustituya *`user input placeholder`* con su propia información.

Para Linux, macOS o Unix:

```
aws docdb-elastic get-cluster-snapshot \
    --snapshot-arn sampleResourceName
```

Para Windows:

```
aws docdb-elastic get-cluster-snapshot ^
    --snapshot-arn sampleResourceName
```

Para ver información sobre todas las instantáneas del clúster elástico que utilizan el AWS CLI, utilice la `list-cluster-snapshots` operación con los siguientes parámetros:

- **`--snapshot-type`**: opcional. El tipo de instantáneas del clúster que se van a devolver. Puede especificar uno de los siguientes valores:
  - `automated`- Devuelva todas las instantáneas del clúster que Amazon DocumentDB haya creado automáticamente para su AWS cuenta.
  - `manual`- Devuelva todas las instantáneas del clúster que haya creado manualmente para su cuenta. AWS
  - `shared`- Devuelve todas las instantáneas de clústeres manuales que se hayan compartido en tu AWS cuenta.
  - `public`: se devuelven todas las instantáneas del clúster que se han marcado como públicas.
- **`--next-token`**: opcional. Un token de paginación opcional proporcionado por una solicitud anterior. Si se especifica este parámetro, la respuesta solo incluye registros más allá del token, hasta el valor especificado por `max-results`.
- **`--max-results`**: opcional. El número máximo de registros que se debe incluir en la respuesta. Si el número de registros es superior al valor `max-results` especificado, se incluye en la respuesta un token de paginación (`next-token`) que se conoce como marcador, de modo que se pueda recuperar el resto de resultados.

- Predeterminado: 100
- Mínimo = 20, máximo = 100

Para utilizar el ejemplo siguiente, sustituya *user input placeholder* con su propia información.

Para Linux, macOS o Unix:

```
aws docdb-elastic list-cluster-snapshots \
    --snapshot-type  value \
    --next-token  value \
    --max-results 50
```

Para Windows:

```
aws docdb-elastic list-cluster-snapshots ^
    --snapshot-type  value ^
    --next-token  value ^
    --max-results 50
```

Restauración de un clúster desde una instantánea

En esta sección, explicamos cómo restaurar un clúster elástico a partir de una instantánea, utilizando las instrucciones siguientes Consola de administración de AWS o AWS CLI siguiendo estas instrucciones.

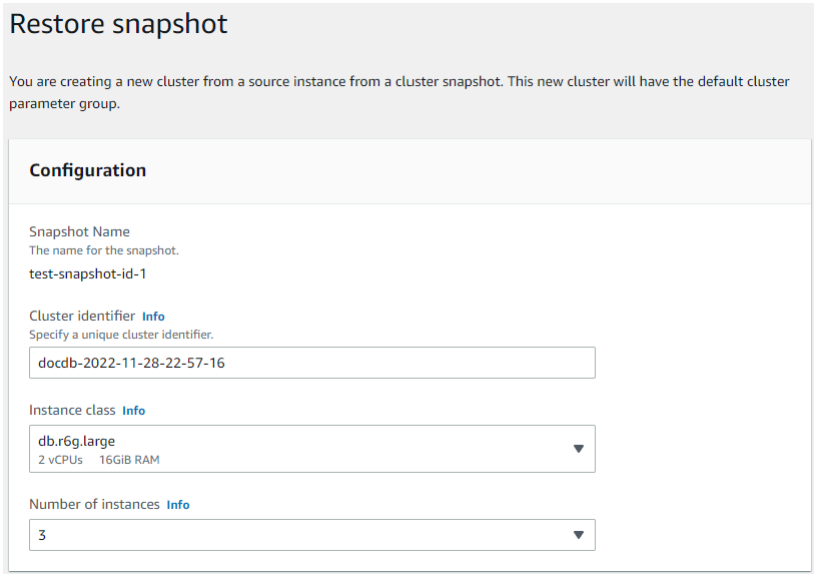
Using the Consola de administración de AWS

Para restaurar un clúster elástico a partir de una instantánea utilizando la Consola de administración de AWS:

1. Inicie sesión en la Consola de administración de AWS de Amazon DocumentDB y ábrala.
2. En el panel de navegación, elija Snapshots (Instantáneas).

> **Tip**
>
> Si no ve el panel de navegación del lado izquierdo de la pantalla, seleccione el icono de menú en la esquina superior izquierda del panel de navegación.

3. Seleccione el botón situado a la izquierda de la instantánea que desea utilizar para restaurar un clúster, en la columna Identificador de instantánea.
4. En Acciones, elija Restaurar.



5. En la página Restaurar la instantánea, introduzca un nombre para el nuevo clúster en el campo identificador del clúster.

> **Note**
>
> Para cualquier restauración manual de instantáneas, debe crear un clúster nuevo.

6. En el campo Nube privada virtual (VPC), elija una VPC de la lista desplegable.
7. Para las subredes y los grupos de seguridad de VPC, puede usar los valores predeterminados o seleccionar tres subredes de su elección y hasta tres grupos de seguridad de VPC (uno como mínimo).
8. Si está satisfecho con la configuración del clúster, elija Restore cluster (Restaurar clúster) y espere mientras el clúster se restaura.

Using the AWS CLI

Para restaurar un clúster elástico a partir de una instantánea mediante la AWS CLI, utilice la `restore-cluster-from-snapshot` operación con los siguientes parámetros:

- **`--cluster-name`**: obligatorio. El nombre actual del clúster elástico tal como se ingresó durante la creación o se modificó por última vez.

- **`--snapshot-arn`**: obligatorio. El identificador del ARN de la instantánea que se utiliza para restaurar el clúster.
- **`--vpc-security-group-ids`**: opcional. Uno o más grupos de seguridad de Amazon EC2 y Amazon Virtual Private Cloud (VPC) para asociarlos al clúster.
- **`--kms-key-id`**: opcional. Configure el identificador de la clave de KMS de un clúster cifrado.

  El identificador de clave de KMS es el nombre de recurso de Amazon (ARN) de la clave de AWS KMS cifrado. Si está creando un clúster con la misma cuenta de Amazon Web Services a la que pertenece la clave de cifrado de KMS utilizada para cifrar el clúster nuevo, puede utilizar el alias de la clave de KMS en lugar del ARN para la clave de cifrado de KMS.

  Si no se especifica ninguna clave de cifrado KmsKeyId y el `StorageEncrypted` parámetro es verdadero, Amazon DocumentDB utiliza la clave de cifrado predeterminada.
- **`--subnet-ids`**: opcional. ID de subred de red.

En el siguiente ejemplo, sustituya cada una *`user input placeholder`* por su propia información.

Para Linux, macOS o Unix:

```
aws docdb-elastic restore-cluster-from-snapshot \
     --cluster-name elastic-sample-cluster \
     --snapshot-arn sampleResourceName \
     --vpc-security-group-ids value ec-65f40350 \
     --kms-key-id arn:aws:docdb-elastic:us-east-1:477568257630:cluster/
b9f1d489-6c3e-4764-bb42-da62ceb7bda2 \
     --subnet-ids subnet-9253c6a3, subnet-9f1b5af9
```

Para Windows:

```
aws docdb-elastic restore-cluster-from-snapshot ^
     --cluster-name elastic-sample-cluster ^
     --snapshot-arn sampleResourceName ^
     --vpc-security-group-ids value ec-65f40350 ^
     --kms-key-id arn:aws:docdb-elastic:us-east-1:477568257630:cluster/
b9f1d489-6c3e-4764-bb42-da62ceb7bda2 ^
     --subnet-ids subnet-9253c6a3, subnet-9f1b5af9
```

Copia de una instantánea de un clúster elástico

En Amazon DocumentDB, puede copiar instantáneas manuales y automáticas de un clúster elástico en la misma región y dentro de la misma cuenta. En esta sección, explicamos cómo copiar una instantánea de un clúster elástico mediante la tecla Consola de administración de AWS o AWS CLI.

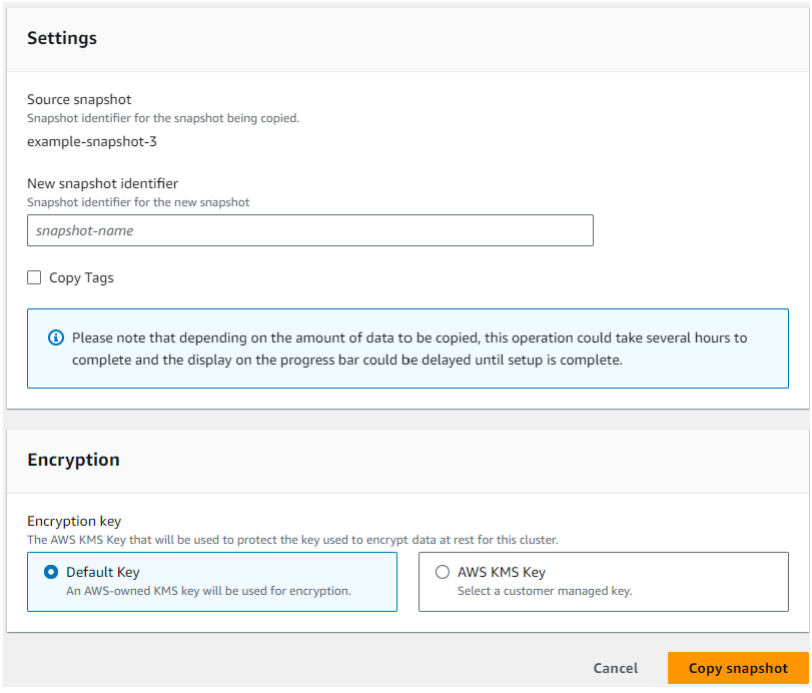
Using the Consola de administración de AWS

Para copiar una instantánea de un clúster elástico mediante Consola de administración de AWS:

1. Inicie sesión en la Consola de administración de AWS de Amazon DocumentDB y ábrala.
2. En el panel de navegación, elija Snapshots (Instantáneas).

> **Tip**
>
> Si no ve el panel de navegación del lado izquierdo de la pantalla, seleccione el icono de menú en la esquina superior izquierda del panel de navegación.

3. Seleccione el botón situado a la izquierda de la instantánea que desea copiar en la columna Identificador de la instantánea.
4. Seleccione Acciones y, a continuación, Copiar.



5. En Identificador de la nueva instantánea, escriba un nombre para la instantánea nueva.

6. En Copiar etiquetas, active la casilla si desea copiar todas las etiquetas de la instantánea del clúster elástico de origen a la instantánea del clúster elástico de destino.
7. Para el cifrado, elija una clave de AWS KMS predeterminada o una clave de KMS de su elección. La segunda opción le permite seleccionar una clave de KMS existente que ya haya creado o crear una nueva.
8. Seleccione Copiar instantánea cuando haya terminado.

Using the AWS CLI

Para copiar una instantánea de un clúster elástico mediante el AWS CLI, utilice la `copy-cluster-snapshot` operación con los siguientes parámetros:

- **`--source-db-cluster-snapshot-identifier`**: obligatorio. El identificador de la instantánea del clúster elástico existente que se está copiando. Debe existir la instantánea del clúster elástico y tener el estado Disponible. Este parámetro no distingue entre mayúsculas y minúsculas.
- **`--target-db-cluster-snapshot-identifier`**: obligatorio. El identificador de la nueva instantánea del clúster elástico que se va a crear a partir de la instantánea del clúster existente. Este parámetro no distingue entre mayúsculas y minúsculas.

  Restricciones relativas a la nomenclatura de instantáneas de destino:
  - No se puede coincidir con el nombre de una instantánea existente.
  - Debe tener [1-63] letras, números o guiones.
  - El primer carácter debe ser una letra.
  - No puede terminar con un guion ni contener dos guiones consecutivos.

Para utilizar el ejemplo siguiente, sustituya *`user input placeholder`* con su propia información.

Para Linux, macOS o Unix:

```
aws docdb-elastic copy-cluster-snapshot \
     --source-cluster-snapshot-arn <sample ARN> \
     --target-cluster-snapshot-name my-target-copied-snapshot
```

Para Windows:

```
aws docdb-elastic copy-cluster-snapshot ^
     --source-cluster-snapshot-arn <sample ARN> ^
     --target-cluster-snapshot-name my-target-copied-snapshot
```

Eliminar una instantánea de un clúster elástico

En esta sección, explicamos cómo eliminar una instantánea de un clúster elástico mediante la tecla Consola de administración de AWS o AWS CLI.

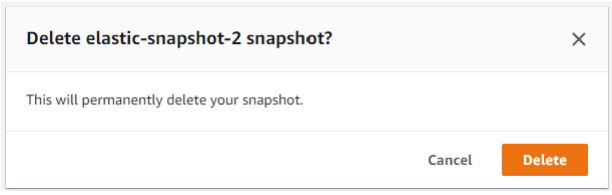
Using the Consola de administración de AWS

Para restaurar un clúster elástico a partir de una instantánea utilizando la Consola de administración de AWS:

1. Inicie sesión en la Consola de administración de AWS de Amazon DocumentDB y ábrala.
2. En el panel de navegación, elija Snapshots (Instantáneas).

> **Tip**
>
> Si no ve el panel de navegación del lado izquierdo de la pantalla, seleccione el icono de menú en la esquina superior izquierda del panel de navegación.

3. Seleccione el botón situado a la izquierda de la instantánea que desea utilizar para restaurar un clúster, en la columna Identificador de instantánea.
4. Elija Acciones y, a continuación, elija Eliminar.



5. En el cuadro de diálogo Eliminar la instantánea “snapshot-name”, seleccione Eliminar.

Using the AWS CLI

Para eliminar una instantánea de un clúster elástico mediante el AWS CLI, utilice la `delete-cluster-snapshot` operación con los siguientes parámetros:

- **`--snapshot-arn`**: obligatorio. El identificador del ARN de la instantánea que se utiliza para restaurar el clúster.

En el siguiente ejemplo, sustituya cada *`user input placeholder`* una por su propia información.

Para Linux, macOS o Unix:

```
aws docdb-elastic delete-cluster-snapshot \
     --snapshot-arn sampleResourceName
```

Para Windows:

```
aws docdb-elastic delete-cluster-snapshot ^
     --snapshot-arn sampleResourceName
```

Administración de una copia de seguridad automática de una instantánea de un clúster elástico

Amazon DocumentDB toma instantáneas diarias de los clústeres elásticos. Puede especificar la ventana de copia de seguridad preferida y el periodo de retención de la copia de seguridad en una configuración de instantáneas de clúster elástico nueva o existente. En esta sección, explicamos cómo configurar los parámetros de copia de seguridad automática en una instantánea de un clúster elástico, utilizando la tecla Consola de administración de AWS o AWS CLI.

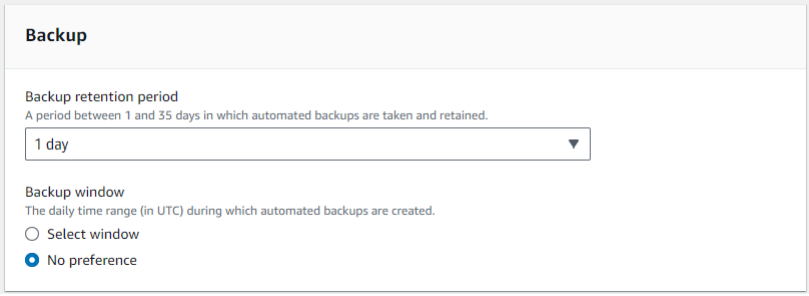
Using the Consola de administración de AWS

Para configurar una copia de seguridad automática para una nueva instantánea de un clúster elástico mediante Consola de administración de AWS:

1. Inicie sesión en la Consola de administración de AWS de Amazon DocumentDB y ábrala.
2. En el panel de navegación, seleccione Clusters (Clústeres).

> **Tip**
>
> Si no ve el panel de navegación del lado izquierdo de la pantalla, seleccione el icono de menú en la esquina superior izquierda del panel de navegación.

3. Seleccione el botón situado a la izquierda del clúster para el que desea cambiar la configuración de copia de seguridad en la columna Identificador del clúster.
4. Elija Acciones y, a continuación, Modificar.
5. En la sección Copia de seguridad, edite los campos de acuerdo con los requisitos de copia de seguridad.



   a. Periodo de retención de copias de seguridad: en la lista, elija el número de días que se deben conservar las copias de seguridad automáticas de este clúster antes de eliminarlas.
   b. Periodo de copia de seguridad: especifique la hora del día en que Amazon DocumentDB debe hacer las copias de seguridad de este clúster y la duración de las mismas.
      i. Elija Seleccionar periodo si desea configurar la hora y la duración de la creación de las copias de seguridad.

         Hora de inicio: en la primera lista, elija la hora de inicio (UTC) para las copias de seguridad automáticas. En la segunda lista, elija el minuto de la hora en que desea que comiencen las copias de seguridad automáticas.

         Duración: en la lista, elija el número de horas que se deben asignar para crear las copias de seguridad automáticas.
      ii. Seleccione Sin preferencia si desea que Amazon DocumentDB elija la hora y la duración de la creación de las copias de seguridad.
6. Elija Modificar clúster cuando haya terminado.

Using the AWS CLI

Para configurar una copia de seguridad automática para una nueva instantánea de un clúster elástico mediante el AWS CLI, utilice la `create-cluster-snapshot` operación con los siguientes parámetros:

- **`--preferred-backup-window`**: opcional. El intervalo de tiempo diario preferido durante el que se crean las copias de seguridad automatizadas. El valor predeterminado es un período de 30 minutos seleccionado al azar de un bloque de tiempo de 8 horas para cada uno Región de AWS.

  Restricciones:

  - Tiene que tener el formato `hh24:mi-hh24:mi`.
  - Debe indicarse en Tiempo universal coordinado (UTC).
  - No debe entrar en conflicto con la ventana de mantenimiento preferida.
  - Debe durar al menos 30 minutos.
- **`--backup-retention-period`**: opcional. El número de días durante los que se retienen las copias de seguridad automatizadas. El valor predeterminado es 1.

  Restricciones:

  - Debe especificar un valor mínimo de 1.
  - El intervalo va de 1 a 35.

> **Note**
>
> Las copias de seguridad automatizadas solo se hacen cuando el clúster tenga el estado "activo".

> **Note**
>
> También puede modificar los parámetros `preferred-backup-window` y `backup-retention-period` de un clúster elástico existente mediante el comando `aws docdb-elastic update-cluster`.

Para utilizar el ejemplo siguiente, sustituya *`user input placeholder`* con su propia información.

El siguiente `create-cluster` ejemplo crea el clúster elástico de Amazon DocumentDB *`sample-cluster`* con el período de retención para las copias de seguridad automáticas de *`7`* días y una ventana de copia de seguridad preferida de. *`18:00-18:30 UTC`*

Para Linux, macOS o Unix:

```
aws docdb-elastic create-cluster \
     --cluster-name sample-cluster \
     --shard-capacity 2 \
     --shard-count 2 \
     --admin-user-name SampleAdmin \
     --auth-type PLAIN_TEXT \
     --admin-user-password SamplePass123! \
     --preferred-backup-window 18:00-18:30 \
     --backup-retention-period 7
```

Para Windows:

```
aws docdb-elastic create-cluster ^
     --cluster-name sample-cluster ^
     --shard-capacity 2 ^
     --shard-count 2 ^
     --admin-user-name SampleAdmin ^
     --auth-type PLAIN_TEXT ^
     --admin-user-password SamplePass123! ^
     --preferred-backup-window 18:00-18:30 ^
     --backup-retention-period 7
```

Detención e inicio de un clúster elástico de Amazon DocumentDB

La detención e inicio de los clústeres elásticos de Amazon DocumentDB puede ayudarlo a administrar los costos de entornos de desarrollo y pruebas. En lugar de crear y eliminar clústeres elásticos cada vez que utilice Amazon DocumentDB, puede detener temporalmente el clúster cuando ya no es necesario. A continuación, puede iniciarlo de nuevo cuando reanude sus pruebas.

Temas

- Información general de detención e inicio de un clúster elástico
- Operaciones que puede llevar a cabo en un clúster elástico detenido

Información general de detención e inicio de un clúster elástico

Durante los periodos en los que no necesite un clúster elástico de Amazon DocumentDB, puede detener el clúster. A continuación, puede volver a iniciar el clúster en cualquier momento que

necesite usarlo. El inicio y la detención simplifican los procesos de configuración y eliminación de clústeres elásticos usados para desarrollo, pruebas o actividades similares que no requieren disponibilidad continua. Puede detener e iniciar un clúster elástico con Consola de administración de AWS o AWS CLI con una sola acción.

Aunque el clúster elástico se detenga, el volumen de almacenamiento del clúster permanece sin cambios. Solo se le cobrará el almacenamiento, las instantáneas manuales y el almacenamiento de la copia de seguridad automática dentro de su intervalo de retención especificado. Después de siete días, Amazon DocumentDB inicia automáticamente el clúster elástico para que no pierda las actualizaciones de mantenimiento necesarias. Cuando el clúster se inicie después de siete días, se le comenzará a cobrar por el uso del clúster elástico de nuevo. Cuando el clúster se detenga, no podrá consultar el volumen de almacenamiento, ya que la consulta requiere que el clúster esté disponible.

Cuando se detiene un clúster elástico de Amazon DocumentDB, no se pueden modificar en modo alguno. Esto incluye la eliminación del clúster.

Using the Consola de administración de AWS

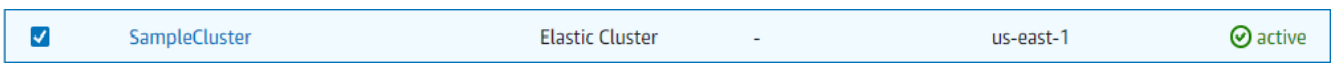
El procedimiento siguiente le muestra cómo detener un clúster elástico en un estado disponible o iniciar un clúster elástico detenido.

Detención o inicio de un clúster elástico de Amazon DocumentDB

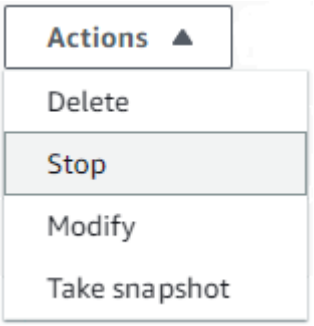
1. Inicie sesión en y abra la Consola de administración de AWS consola de Amazon DocumentDB en https://console.aws.amazon.com /docdb.
2. En el panel de navegación, seleccione Clusters (Clústeres).

   > **Tip**
   >
   > Si no ve el panel de navegación del lado izquierdo de la pantalla, seleccione el icono de menú
   > (≡)
   > en la esquina superior izquierda de la página.

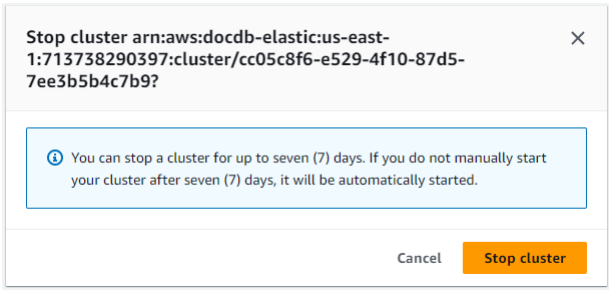
3. En la lista de clústeres, elija el botón situado a la izquierda del nombre del clúster que quiera detener o iniciar.



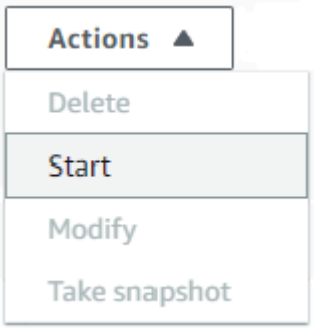
4. Elija Actions (Acciones) y, a continuación, elija la acción que desea realizar en el clúster.
   - Si desea detener el clúster y el clúster está disponible:
     a. Elija Detener.



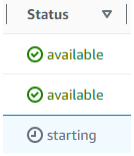
     b. En el cuadro de diálogo de confirmación, seleccione Detener clúster parar confirmar que desea detener el clúster elástico o elija Cancelar para mantener el clúster en ejecución.



   - Si desea iniciar el clúster y este se detiene, seleccione Start (Iniciar).



5. Supervise el estado del clúster elástico. Si ha iniciado el clúster, podrá volver a utilizarlo cuando esté Disponible. Para obtener más información, consulte Determinación del estado de un clúster.



Using the AWS CLI

En los ejemplos de código siguientes se muestra cómo detener un clúster elástico en un estado activo o disponible o iniciar un clúster elástico detenido.

Para detener un clúster elástico mediante el AWS CLI, utilice la operación. `stop-cluster` Para iniciar un clúster detenido, utilice la operación `start-cluster`. En ambas operaciones se utiliza el parámetro `--cluster-arn`.

Parámetro

- **`--cluster-arn`**: obligatorio. El identificador ARN del clúster elástico que desee detener o iniciar.

Example — Para detener un clúster elástico mediante el AWS CLI

Para utilizar el ejemplo siguiente, sustituya *`user input placeholder`* con su propia información.

El siguiente código detiene el clúster elástico con un ARN de `arn:aws:docdb-elastic:us-east-1:477568257630:cluster/b9f1d489-6c3e-4764-bb42-da62ceb7bda2`.

> **Note**
>
> El estado del clúster elástico debe ser activo o disponible.

Para Linux, macOS o Unix:

```
aws docdb-elastic stop-cluster \
   --cluster-arn arn:aws:docdb-elastic:us-east-1:477568257630:cluster/
b9f1d489-6c3e-4764-bb42-da62ceb7bda2
```

Para Windows:

```
aws docdb-elastic stop-cluster ^
   --cluster-arn arn:aws:docdb-elastic:us-east-1:477568257630:cluster/
b9f1d489-6c3e-4764-bb42-da62ceb7bda2
```

Example — Para iniciar un clúster elástico mediante el AWS CLI

Para utilizar el ejemplo siguiente, sustituya *user input placeholder* con su propia información.

El siguiente código inicia el clúster elástico con un ARN de `arn:aws:docdb-elastic:us-east-1:477568257630:cluster/b9f1d489-6c3e-4764-bb42-da62ceb7bda2`.

> **Note**
>
> El clúster elástico debe estar detenido actualmente.

Para Linux, macOS o Unix:

```
aws docdb-elastic start-cluster \
   --cluster-arn arn:aws:docdb-elastic:us-east-1:477568257630:cluster/
b9f1d489-6c3e-4764-bb42-da62ceb7bda2
```

Para Windows:

```
aws docdb-elastic start-cluster ^
   --cluster-arn arn:aws:docdb-elastic:us-east-1:477568257630:cluster/
b9f1d489-6c3e-4764-bb42-da62ceb7bda2
```

Operaciones que puede llevar a cabo en un clúster elástico detenido

No se puede modificar la configuración de un clúster elástico de Amazon DocumentDB mientras el clúster esté detenido. Debe iniciar el clúster antes de realizar cualquier tarea administrativa de ese tipo.

Amazon DocumentDB aplica cualquier mantenimiento programado a su clúster elástico detenido solo después de que se vuelva a iniciar. Después de siete días, Amazon DocumentDB inicia automáticamente un clúster elástico detenido para que no se quede demasiado rezagado en su estado de mantenimiento. Cuando el clúster elástico se reinicie, se le comenzará a cobrar por las particiones en el clúster de nuevo.

Cuando un clúster elástico está detenido, Amazon DocumentDB no hace copias de seguridad automatizadas ni amplía el periodo de retención de copia de seguridad.

Mantenimiento de clústeres elásticos de Amazon DocumentDB

Temas

- Visualización de las acciones de mantenimiento pendientes del clúster elástico
- Actualizaciones del motor de clústeres elásticos
- Actualizaciones del sistema operativo para los clústeres elásticos

Amazon DocumentDB realiza tareas de mantenimiento periódicas en los recursos del clúster elástico de Amazon DocumentDB. En la mayoría de los casos, el mantenimiento incluye actualizaciones del motor de base de datos (mantenimiento de clústeres elásticos) o del sistema operativo subyacente del clúster elástico (actualizaciones del sistema operativo). Las actualizaciones del motor de base de datos son parches necesarios e incluyen correcciones de seguridad, correcciones de errores y mejoras en el motor de base de datos. Si bien la mayoría de los parches del sistema operativo son opcionales, si no los aplica durante un tiempo, es posible que el parche sea necesario y se aplique automáticamente para mantener su postura de seguridad. Por lo tanto, le recomendamos que aplique las actualizaciones del sistema operativo a sus clústeres elásticos de Amazon DocumentDB tan pronto como estén disponibles.

Los parches del motor de base de datos requieren que desconecte los clústeres elásticos de Amazon DocumentDB durante un breve plazo de tiempo. Una vez disponibles, estos parches se programan automáticamente para que se apliquen durante un próximo período de mantenimiento programado del clúster elástico de Amazon DocumentDB.

Los clústeres elásticos tienen sus propios períodos de mantenimiento respectivos. Las modificaciones de los clústeres elásticos que haya decidido no aplicar inmediatamente también se aplican durante el período de mantenimiento. De forma predeterminada, cuando crea un clúster elástico, Amazon DocumentDB asigna un período de mantenimiento para el clúster elástico. Puede elegir el período de mantenimiento cuando crea el clúster elástico. También puede modificar los periodos de mantenimiento en cualquier momento para ajustarlos a las prácticas o las programaciones de su empresa. Por lo general, se recomienda elegir periodos de mantenimiento que minimicen la repercusión de las tareas de mantenimiento en la aplicación (por ejemplo, por las noches o durante los fines de semana).

Visualización de las acciones de mantenimiento pendientes del clúster elástico

Para ver si hay disponible una actualización de mantenimiento para un clúster elástico, use la AWS CLI.

Si hay disponible una actualización, puede realizar una de las acciones siguientes:

- Aplace una acción de mantenimiento que esté actualmente programada para el próximo periodo de mantenimiento (solo para los parches del sistema operativo).
- Aplicar inmediatamente las operaciones de mantenimiento.
- Programar las operaciones de mantenimiento para que se inicien durante el siguiente periodo de mantenimiento.
- Programe las acciones de mantenimiento para que se inicien durante el período de aplicación seleccionado.

El periodo de mantenimiento determina el momento en que comienzan las operaciones pendientes, pero no limita su tiempo total de ejecución.

Utilice la siguiente AWS CLI operación para determinar qué acciones de mantenimiento están pendientes. Enumere todas las acciones de mantenimiento pendientes:

```
aws docdb-elastic list-pending-maintenance-actions
```

La salida de esta operación será similar a lo que se indica a continuación (formato JSON):

```
{
'ResourcePendingMaintenanceActions': [
    {
        'ResourceArn': 'string-arn',
        'PendingMaintenanceActionDetails': [
            {
                'Action': 'ENGINE_UPDATE',
                'AutoAppliedAfterDate': 'string',
                'ForcedApplyDate': 'string',
                'OptInStatus': 'string',
                'CurrentApplyDate': 'string',
                'Description': 'string'
            },
        ]
    },
],
'NextToken': 'string'
}
```

Obtenga la acción de mantenimiento pendiente (si la hubiera) en un `resourceArn` dado:

```
aws docdb-elastic get-pending-maintenance-action --resource-arn string-arn
```

La salida de esta operación será similar a lo que se indica a continuación (formato JSON).

```
{
    'ResourcePendingMaintenanceAction': {
        'ResourceArn': 'string-arn',
        'PendingMaintenanceActionDetails': [
            {
                'Action': 'ENGINE_UPDATE',
                'AutoAppliedAfterDate': 'string',
                'ForcedApplyDate': 'string',
                'OptInStatus': 'string',
                'CurrentApplyDate': 'string',
                'Description': 'string'
            }
        ]
    }
}
```

Parámetros:

- `ResourceArn`: el Nombre de recurso de Amazon (ARN) de Amazon DocumentDB del recurso al que se aplica la acción de mantenimiento pendiente.
- `Action`: la acción de mantenimiento pendiente que se aplica a este recurso.

  Valores válidos:

  - `ENGINE_UPDATE`
  - `ENGINE_UPGRADE`
  - `SECURITY_UPDATE`
  - `OS_UPDATE`
  - `MASTER_USER_PASSWORD_UPDATE`
- `AutoAppliedAfterDate`: primer período de mantenimiento después de esta fecha. `NEXT_MAINTENANCE OPT_IN` se ignora en este caso.
- `ForcedApplyDate`: se aplica independientemente del período de mantenimiento. `IMMEDIATE OPT_IN` se ignora en este caso.
- `OptInStatus`: un valor que indica el tipo de solicitud de alta o deshace una solicitud de alta. Una solicitud de alta de tipo `IMMEDIATE` no se puede deshacer.

Valores válidos:

- `IMMEDIATE`: aplicar inmediatamente la acción de mantenimiento.
- `NEXT_MAINTENANCE`: aplicar la acción de mantenimiento durante la siguiente ventana de mantenimiento del recurso.
- `APPLY_ON`: aplicar la acción de mantenimiento en la fecha de aplicación especificada, independientemente del siguiente período de mantenimiento del recurso.
- `UNDO_OPT_IN`: cancelar todas las solicitudes de alta de `NEXT_MAINTENANCE` o `APPLY_ON` existentes.

- `CurrentApplyDate`—Se muestra si lo opt-in-type está`APPLY_ON`.
- `Description`: una descripción de la opción para la acción de mantenimiento.

Actualizaciones del motor de clústeres elásticos

Con Amazon DocumentDB puede elegir el momento en que desea aplicar las operaciones de mantenimiento. Puede indicar cuándo Amazon DocumentDB debe aplicar las actualizaciones mediante la AWS CLI.

Aplique las acciones de mantenimiento pendientes:

```
aws docdb-elastic apply-pending-maintenance-action
--resource-arn string-arn
--apply-action string-enum
--opt-in-type string-enum
[--apply-on string-date-range]
```

Parámetros:

- **`--resource-arn`**: el Nombre de recurso de Amazon (ARN) de Amazon DocumentDB del recurso al que se aplica la acción de mantenimiento pendiente.
- **`--apply-action`**: la acción de mantenimiento pendiente que se aplica a este recurso.

  Valores válidos:

  - `ENGINE_UPDATE`
  - `ENGINE_UPGRADE`
  - `SECURITY_UPDATE`
  - `OS_UPDATE`

  - MASTER_USER_PASSWORD_UPDATE
- **--opt-in-type**: un valor que indica el tipo de solicitud de alta o deshace una solicitud de alta. Una solicitud de alta de tipo IMMEDIATE no se puede deshacer.

  Valores válidos:

  - IMMEDIATE: aplicar inmediatamente la acción de mantenimiento.
  - NEXT_MAINTENANCE: aplicar la acción de mantenimiento durante la siguiente ventana de mantenimiento del recurso.
  - APPLY_ON: aplicar la acción de mantenimiento en la fecha de aplicación especificada, independientemente del siguiente período de mantenimiento del recurso.
  - UNDO_OPT_IN: cancelar todas las solicitudes de alta de NEXT_MAINTENANCE o APPLY_ON existentes.
- **[--apply-on]**: obligatorio si opt-in-type es APPLY_ON. Formato: yyyy/MM/dd HH:mm-yyyy/MM/dd HH:mm (Esta opción usa la hora UTC. La hora de inicio puede ser en cualquier momento futuro, entre un mínimo de 30 minutos y un máximo de 14 días, o la force/apply fecha de la acción pendiente, lo que ocurra primero. (El intervalo de tiempo de inicio a fin puede ser de un mínimo de 30 minutos a un máximo de 8 horas).

La salida de esta operación será similar a lo que se indica a continuación (formato JSON):

```
{
 'ResourcePendingMaintenanceAction': {
        'ResourceArn': 'string-arn',
        'PendingMaintenanceActionDetails': [
            {
                'Action': 'SECURITY_UPDATE',
                'AutoAppliedAfterDate': 'string',
                'ForcedApplyDate': 'string',
                'OptInStatus': 'IMMEDIATE',
                'CurrentApplyDate': 'string',
                'Description': 'string'
            },
        ]
 }
}
```

Parámetros:

- `ResourceArn`: el Nombre de recurso de Amazon (ARN) de Amazon DocumentDB del recurso al que se aplica la acción de mantenimiento pendiente.
- `Action`: la acción de mantenimiento pendiente que se aplica a este recurso.

  Valores válidos:

  - `ENGINE_UPDATE`
  - `ENGINE_UPGRADE`
  - `SECURITY_UPDATE`
  - `OS_UPDATE`
  - `MASTER_USER_PASSWORD_UPDATE`
- `AutoAppliedAfterDate`: primer período de mantenimiento después de esta fecha. `NEXT_MAINTENANCE OPT_IN` se ignora en este caso.
- `ForcedApplyDate`: se aplica independientemente del período de mantenimiento. `IMMEDIATE OPT_IN` se ignora en este caso.
- `OptInStatus`: un valor que indica el tipo de solicitud de alta o deshace una solicitud de alta. Una solicitud de alta de tipo `IMMEDIATE` no se puede deshacer.

  Valores válidos:

  - `IMMEDIATE`: aplicar inmediatamente la acción de mantenimiento.
  - `NEXT_MAINTENANCE`: aplicar la acción de mantenimiento durante la siguiente ventana de mantenimiento del recurso.
  - `APPLY_ON`: aplicar la acción de mantenimiento en la fecha de aplicación especificada, independientemente del siguiente período de mantenimiento del recurso.
  - `UNDO_OPT_IN`: cancelar todas las solicitudes de alta de `NEXT_MAINTENANCE` o `APPLY_ON` existentes.
- `CurrentApplyDate`—Se muestra si opt-in-type es `APPLY_ON` así.
- `Description`: una descripción de la opción para la acción de mantenimiento.

Fechas de aplicación

Cada operación de mantenimiento tiene una fecha de aplicación que encontrará al describir las operaciones de mantenimiento pendientes. Al leer el resultado de las acciones de mantenimiento pendientes del AWS CLI, aparecen tres fechas:

- `CurrentApplyDate`: fecha en la que se aplicará la acción de mantenimiento inmediatamente o en la siguiente ventana de mantenimiento. Si el mantenimiento es opcional, este valor puede ser nulo.
- `ForcedApplyDate`: fecha en la que el mantenimiento se aplicará automáticamente, independientemente del período de mantenimiento.
- `AutoAppliedAfterDate`: fecha a partir de la cual se aplicará el mantenimiento durante el período de mantenimiento del clúster.

Acciones de mantenimiento creadas por el usuario

Como usuario del DBelastic clúster de Amazon Document, puede iniciar actualizaciones en las configuraciones de los clústeres.

Actualización de la contraseña principal del clúster

```
aws docdb-elastic update-cluster
--cluster-arn string-arn
[--admin-user-password string]
[--auth-type string-enum]
[--apply-method string-enum]
[--apply-on string-date-range]
#... other parameters of the API that follow here are not relevant for this
 configuration
```

Parámetros:

- **`--cluster-arn`**: el Nombre de recurso de Amazon (ARN) de Amazon DocumentDB del recurso al que se aplicará la acción de mantenimiento pendiente.
- **`[--admin-user-password]`**: la contraseña asociada al usuario administrador.
- **`[--auth-type]`**: el tipo de autenticación utilizado para determinar dónde buscar la contraseña que se usa para acceder al clúster elástico. Los tipos válidos son `PLAIN_TEXT` o `SECRET_ARN`.
- **`[--apply-method]`**: un valor que especifica el tipo de método que se aplica. Los valores permitidos son `IMMEDIATE` y `APPLY_ON`. El valor predeterminado es `IMMEDIATE`.
- **`[--apply-on]`**: obligatorio si `apply-method` es `APPLY_ON`. Formato: `yyyy/MM/dd HH:mm-yyyy/MM/dd HH:mm` (Esta opción usa la hora UTC. La hora de inicio puede ser en cualquier momento futuro, entre un mínimo de 30 minutos y un máximo de 14 días. El intervalo de tiempo de inicio a fin puede ser de un mínimo de 30 minutos a un máximo de 8 horas).

La salida de esta operación será similar a lo que se indica a continuación (formato JSON):

```
{
 'ResourcePendingMaintenanceAction': {
        'ResourceArn': 'string-arn',
        'PendingMaintenanceActionDetails': [
            {
                'Action': 'MASTER_USER_PASSWORD_UPDATE',
                'OptInStatus': 'APPLY_ON',
                'CurrentApplyDate': 'string',
                'Description': 'string'
            },
        ]
 }
}
```

Cambio de los periodos de mantenimiento de Amazon DocumentDB

El periodo de mantenimiento debe corresponder al momento de mínimo uso y, por tanto, podría ser preciso modificarlo cada cierto tiempo. El clúster elástico deja de estar disponible durante este período solamente si se están aplicando cambios en el sistema (por ejemplo, se está realizando un cambio en la operación de escalado del almacenamiento) y se requiere una interrupción. Solamente dejará de estar disponible durante el tiempo mínimo requerido para realizar los cambios necesarios.

El valor predeterminado es un periodo de 30 minutos seleccionado al azar de un bloque de 8 horas de tiempo para cada región de Amazon Web Services, que tiene lugar un día de la semana de forma aleatoria.

Para cambiar el período de mantenimiento, consulte Modificación de configuraciones de clústeres elásticos.

Actualizaciones del sistema operativo para los clústeres elásticos

En ocasiones, los clústeres elásticos de Amazon DocumentDB requieren actualizaciones del sistema operativo. Amazon DocumentDB actualiza el sistema operativo a una versión más reciente para mejorar el rendimiento de la base de datos y la posición de seguridad general de los clientes. Las actualizaciones del sistema operativo no cambian la versión del motor del clúster elástico de Amazon DocumentDB.

La mayoría de las actualizaciones del sistema operativo para los clústeres elásticos de Amazon DocumentDB son opcionales y no tienen una fecha de aplicación fija. Sin embargo, si no aplica

estas actualizaciones durante un tiempo, es posible que acaben siendo necesarias y se apliquen automáticamente durante el período de mantenimiento de su clúster. Esto ayuda a mantener la posición de seguridad de la base de datos. Para evitar cualquier tiempo de inactividad inesperado, le recomendamos que aplique las actualizaciones del sistema operativo al clúster elástico de Amazon DocumentDB tan pronto como estén disponibles y que establezca el período de mantenimiento del clúster en el momento que le resulte más conveniente según las necesidades de la empresa.

Activación del cifrado de datos en reposo de un clúster elástico de Amazon DocumentDB

Los siguientes temas le ayudan a conocer, crear y supervisar las claves de cifrado AWS Key Management Service para los clústeres elásticos de Amazon DocumentDB:

Temas

- Cómo utilizan las subvenciones los clústeres elásticos de Amazon DocumentDB en AWS KMS
- Crear una clave administrada por el cliente
- Supervisión de las claves de cifrado de clústeres elásticos de Amazon DocumentDB
- Más información

Los clústeres elásticos de Amazon DocumentDB se integran automáticamente con AWS Key Management Service (AWS KMS) para la administración de claves y utilizan un método conocido como cifrado de sobre para proteger los datos. Para obtener más información acerca del cifrado de sobre, consulte Cifrado de sobre en la Guía para desarrolladores de AWS Key Management Service.

Un AWS KMS key es una representación lógica de una clave. La clave de KMS incluye metadatos, como el ID de clave, la fecha de creación, la descripción y el estado de la clave. La clave de KMS también contiene el material de claves utilizado para cifrar y descifrar datos. Para obtener más información acerca de las claves de KMS, consulte AWS KMS keys en la Guía para desarrolladores de AWS Key Management Service.

Los clústeres elásticos de Amazon DocumentDB admiten el cifrado con dos tipos de claves:

- claves propias de AWS: los clústeres elásticos de Amazon DocumentDB utilizan estas claves de forma predeterminada para cifrar automáticamente los datos de identificación personal. No puede ver, administrar ni usar las llaves propiedad de AWS, ni auditar su uso. Sin embargo, no tiene que realizar ninguna acción ni cambiar ningún programa para proteger las claves que cifran

sus datos. Para obtener más información, consulte las claves propiedad de AWS en la Guía para desarrolladores de AWS Key Management Service.

- Claves administradas por el cliente: AWS KMS keys simétricas que usted ha creado, posee y administra. Como usted tiene el control total de este cifrado, puede realizar dichas tareas como:
  - Establecer y mantener políticas de claves
  - Establecer y mantener concesiones y políticas de IAM
  - Habilitar y deshabilitar políticas de claves
  - Rotar el material criptográfico
  - Agregar etiquetas.
  - Crear alias de clave
  - Programar la eliminación de claves

  Para obtener más información, consulte las claves administradas por el cliente en la Guía para desarrolladores de AWS Key Management Service.

> **Important**
>
> Debe utilizar una clave de cifrado de KMS simétrica para cifrar el clúster, ya que Amazon DocumentDB solo admite claves de cifrado de KMS de cifrado simétricas. No utilice una CMK asimétrica para intentar cifrar los datos de los clústeres elásticos de Amazon DocumentDB. Para obtener más información, consulte claves asimétricas de AWS KMS en la Guía para desarrolladores de AWS Key Management Service.
> Si Amazon DocumentDB ya no puede obtener acceso a la clave de cifrado de un clúster, por ejemplo, cuando se revoca el acceso a una clave, el clúster cifrado entra en un estado terminal. En este caso, solo puede restaurar el clúster desde una copia de seguridad. Para Amazon DocumentDB, las copias de seguridad siempre están habilitadas durante 1 día. Además, si deshabilita la clave de un clúster cifrado de Amazon DocumentDB, eventualmente perderá el acceso de lectura y escritura a ese clúster. Cuando Amazon DocumentDB encuentra una instancia que está cifrada con una clave a la que no tiene acceso, pone el clúster en un estado terminal. En dicho estado, el clúster ya no está disponible y no es posible recuperar su estado actual. Para restaurar el clúster, debe volver a activar el acceso a la clave de cifrado para Amazon DocumentDB y después restaurar el clúster a partir de una copia de seguridad.

> **Important**
>
> No puede cambiar la clave KMS de un clúster cifrado después de haberlo creado. Asegúrese de determinar los requisitos de clave de cifrado antes de crear el clúster elástico cifrado.

Cómo utilizan las subvenciones los clústeres elásticos de Amazon DocumentDB en AWS KMS

Los clústeres elásticos de Amazon DocumentDB requieren una concesión para utilizar la clave administrada por el cliente.

Cuando crea un clúster cifrado con una clave administrada por el cliente, los clústeres elásticos de Amazon DocumentDB crean una concesión en su nombre mediante el envío de la `CreateGrant` solicitud a AWS KMS. Las concesiones en AWS KMS se utilizan para otorgar a los clústeres elásticos de Amazon DocumentDB acceso a una clave KMS en una cuenta de cliente.

Los clústeres elásticos de Amazon DocumentDB necesitan la concesión para utilizar la clave administrada por el cliente para las siguientes operaciones internas:

- Enviar solicitudes de `DescribeKey` a AWS KMS para comprobar que el ID de clave de KMS simétrico administrado por el cliente, introducido al crear un rastreador o una colección de geocercas, es válido.
- Enviar solicitudes de `GenerateDataKey` a AWS KMS para generar claves de datos cifradas por su clave gestionada por el cliente.
- Enviar solicitudes de `Decrypt` a AWS KMS para descifrar las claves de datos cifradas, para que puedan usarse para cifrar sus datos.
- Puede revocar el acceso a la concesión o eliminar el acceso del servicio a la clave administrada por el cliente en cualquier momento. Si lo hace, los clústeres elásticos de Amazon DocumentDB no podrán acceder a ninguno de los datos cifrados por la clave administrada por el cliente, lo que afectará a las operaciones que dependen de esos datos.

Crear una clave administrada por el cliente

Puede crear una clave administrada por el cliente a través de la Consola de administración de AWS o la API de AWS KMS.

Creación de claves simétricas administradas por el cliente

Siga los pasos para crear una clave simétrica gestionada por el cliente que se indican en la Guía para desarrolladores de AWS Key Management Service.

Política de claves

Las políticas de clave controlan el acceso a la clave administrada por el cliente. Cada clave administrada por el cliente debe tener exactamente una política de clave, que contiene instrucciones que determinan quién puede usar la clave y cómo puede utilizarla. Cuando crea la clave administrada por el cliente, puede especificar una política de clave. Para obtener más información, consulte la información de acceso a la clave de KMS que se encuentra en la descripción general de AWS Key Management Service de la Guía para desarrolladores de AWS Key Management Service.

Para utilizar la clave administrada por el cliente con los recursos de los clústeres elásticos de Amazon DocumentDB, se deben permitir las siguientes operaciones de API en la política de claves:

- `kms:CreateGrant` – agrega una concesión a una clave administrada por el cliente. Otorga el acceso de control a una clave KMS específica, que permite acceder a las operaciones de concesión que requiere Amazon Location Service. Para obtener más información sobre las concesiones, consulte Uso de concesionesAWS KMS en la Guía para desarrolladores de AWS Key Management Service.
- `kms:DescribeKey`: proporciona los detalles de la clave administrada por el cliente para permitir que Docdb Elastic valide la clave.
- `kms:Decrypt`: permite a Docdb Elastic utilizar la clave de datos cifrados almacenada para acceder a los datos cifrados.
- `kms:GenerateDataKey`: permite a Docdb Elastic generar una clave de datos cifrada y almacenarla, ya que la clave de datos no se utiliza inmediatamente para cifrar.

Para obtener más información, consulte los permisos de los servicios de AWS en las políticas de claves y la Solución de problemas de acceso a las claves en la Guía para desarrolladores de AWS Key Management Service.

Restricción del acceso a las claves gestionadas por el cliente mediante políticas de IAM

Además de las políticas clave de KMS, también puede restringir los permisos de clave de KMS en una política de IAM.

Puede hacer que la política de IAM sea más estricta de varias maneras. Por ejemplo, para permitir que la clave administrada por el cliente se utilice solo para solicitudes que se originen en clústeres elásticos de Amazon DocumentDB, puede utilizar la `kms:ViaService`clave de condición con el valor `docdb-elastic.<region-name>.amazonaws.com`.

Para obtener más información, consulte Permitir que los usuarios de otras cuentas utilicen una clave de KMS en la Guía para desarrolladores de AWS Key Management Service.

Supervisión de las claves de cifrado de clústeres elásticos de Amazon DocumentDB

Cuando utiliza una clave administrada por el cliente de AWS KMS key con sus recursos de Docdb Elastic, puede utilizar AWS CloudTrail o Registros de Amazon CloudWatch para hacer un seguimiento de las solicitudes que Docdb Elastic envía a AWS KMS.

Los siguientes ejemplos son eventos AWS CloudTrail para `CreateGrant`, `GenerateDataKeyWithoutPlainText`, `Decrypt`, y `DescribeKey` para monitorear las operaciones de AWS KMS key por parte de los clústeres elásticos de Amazon DocumentDB para acceder al cifrado de datos por su clave administrada por el cliente:

CreateGrant

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE",
                "arn": "arn:aws:iam::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Sampleuser01"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-05-09T23:04:20Z",
```

```
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "docdb-elastic.amazonaws.com"
    },
    "eventTime": "2023-05-09T23:55:48Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateGrant",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "docdb-elastic.amazonaws.com",
    "userAgent": "docdb-elastic.amazonaws.com",
    "requestParameters": {
        "retiringPrincipal": "docdb-elastic.us-east-1.amazonaws.com",
        "granteePrincipal": "docdb-elastic.us-east-1.amazonaws.com",
        "operations": [
            "Decrypt",
            "Encrypt",
            "GenerateDataKey",
            "GenerateDataKeyWithoutPlaintext",
            "ReEncryptFrom",
            "ReEncryptTo",
            "CreateGrant",
            "RetireGrant",
            "DescribeKey"
        ],
        "keyId": "arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    },
    "responseElements": {
        "grantId":
 "0ab0ac0d0b000f00ea00cc0a0e00fc00bce000c000f0000000c0bc0a0000aaafSAMPLE",
        "keyId": "arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    },
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": false,
    "resources": [
        {
            "accountId": "AWS Internal",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
```

```
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

GenerateDataKey

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE",
                "arn": "arn:aws:iam::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Sampleuser01"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-05-10T18:02:59Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "docdb-elastic.amazonaws.com"
    },
    "eventTime": "2023-05-10T18:03:25Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "docdb-elastic.amazonaws.com",
    "userAgent": "docdb-elastic.amazonaws.com",
    "requestParameters": {
        "keySpec": "AES_256",
        "keyId": "arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
```

```
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "AWS Internal",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Decrypt

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE",
                "arn": "arn:aws:iam::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Sampleuser01"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-05-10T18:05:49Z",
                "mfaAuthenticated": "false"
            }
        },
```

```
        "invokedBy": "docdb-elastic.amazonaws.com"
    },
    "eventTime": "2023-05-10T18:06:19Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "docdb-elastic.amazonaws.com",
    "userAgent": "docdb-elastic.amazonaws.com",
    "requestParameters": {
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT"
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "AWS Internal",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

DescribeKey

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE",
```

```
                "arn": "arn:aws:iam::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Sampleuser01"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-05-09T23:04:20Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "docdb-elastic.amazonaws.com"
    },
    "eventTime": "2023-05-09T23:55:48Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "DescribeKey",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "docdb-elastic.amazonaws.com",
    "userAgent": "docdb-elastic.amazonaws.com",
    "requestParameters": {
        "keyId": "alias/SampleKmsKey"
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "AWS Internal",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


Más información

Los siguientes recursos proporcionan más información sobre cifrado de datos en reposo:

- Para obtener más información acerca de conceptos de AWS KMS, consulte Conceptos básicos de AWS Key Management Service en la Guía para desarrolladores de AWS Key Management Service.
- Para obtener más información sobre la seguridad de AWS KMS, consulte Prácticas de seguridad recomendadas para AWS Key Management Service en la guía para desarrolladores de AWS Key Management Service.

Roles vinculados a servicios en clústeres elásticos

Los clústeres elásticos de Amazon DocumentDB utilizan funciones vinculadas a AWS Identity and Access Management servicios (IAM). Un rol vinculado a un servicio es un tipo único de rol de IAM que está vinculado directamente a los clústeres elásticos de Amazon DocumentDB. Los clústeres elásticos de Amazon DocumentDB predefinen las funciones vinculadas a servicios e incluyen todos los permisos que el servicio necesita para llamar a AWS otros servicios en su nombre.

Un rol vinculado a servicios simplifica la configuración de Amazon DocumentDB porque ya no tendrá que agregar manualmente los permisos necesarios. Los clústeres elásticos de Amazon DocumentDB definen los permisos de sus roles vinculados al servicio y, a menos que esté definido de otra manera, solo los clústeres elásticos de Amazon DocumentDB pueden asumir sus roles. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se pueda asociar a ninguna otra entidad de IAM. Las funciones se pueden eliminar únicamente después de eliminar primero sus recursos relacionados. De esta forma, se protegen los recursos de los clústeres elásticos de Amazon DocumentDB, ya que se evita que se puedan eliminar accidentalmente permisos de acceso a los recursos.

Para obtener información sobre otros servicios que admiten roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM y busque los servicios que muestran Sí en la columna Rol vinculado a servicios. Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado al servicio en cuestión.

Permisos de rol vinculado a servicios para clústeres elásticos

Los clústeres elásticos de Amazon DocumentDB utilizan el rol vinculado al servicio denominado para permitir que los clústeres elásticos de `AWS ServiceRoleForDocDB-Elastic` Amazon DocumentDB llamen a los AWS servicios en nombre de sus clústeres.

Este rol vinculado al servicio tiene una política de permisos adjunta llamada `AmazonDocDB-ElasticServiceRolePolicy` que le otorga permisos para operar en su cuenta. La política de

permisos del rol permite que los clústeres elásticos de Amazon DocumentDB realicen las siguientes acciones en los recursos especificados:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": [
                        "AWS/DocDB-Elastic"
                    ]
                }
            }
        }
    ]
}
```

> **Note**
>
> Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Si aparece el siguiente mensaje de error: “No se puede crear el recurso. Verifique que tiene permiso para crear el rol vinculado al servicio. De lo contrario, espere y vuelva a intentarlo más tarde”., asegúrese de tener habilitados los siguientes permisos:

```
{
"Action": "iam:CreateServiceLinkedRole",
```

```
    "Effect": "Allow",
    "Resource": "arn:aws:iam::*:role/aws-service-role/docdb-elastic.amazonaws.com/
AWSServiceRoleForDocDB-Elastic",
    "Condition": {
"StringLike": {
"iam:AWSServiceName":"docdb-elastic.amazonaws.com"
        }
    }
}
```

Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de la gestión de identidades y accesos de AWS .

Creación de un rol vinculado a servicio para los clústeres elásticos de Amazon DocumentDB

No necesita crear manualmente un rol vinculado a servicios. Cuando crea una instancia de base de datos, los clústeres elásticos de Amazon DocumentDB vuelven a crear por usted el rol vinculado al servicio.

Edición de un rol vinculado a servicio para los clústeres elásticos de Amazon DocumentDB

Los clústeres elásticos de Amazon DocumentDB no permiten editar el rol vinculado a servicios de `AWS ServiceRoleForDocDB-Elastic`. Después de crear un rol vinculado al servicio, no podrá cambiar el nombre del rol, ya que varias entidades podrían hacer referencia al rol. Sin embargo, sí puede editar la descripción del rol con IAM. Para obtener más información, consulte Edición de roles vinculados a servicios en la Guía del usuario de la gestión de identidades y accesos de AWS .

Eliminación de un rol vinculado a servicio para los clústeres elásticos de Amazon DocumentDB

Si ya no necesita utilizar una característica o servicio que requiere un rol vinculado a un servicio, le recomendamos que elimine dicho rol. De esta forma no tiene una entidad no utilizada que no se monitoree ni mantenga de forma activa. Sin embargo, debe eliminar todos los clústeres para poder eliminar el rol vinculado al servicio.

Limpiar un rol vinculado a servicios

Antes de poder utilizar IAM para eliminar un rol vinculado a un servicio, primero debe confirmar que dicho rol no tiene sesiones activas y eliminar los recursos que utiliza.

Para comprobar si el rol vinculado a un servicio tiene una sesión activa en la consola de IAM:

1. Inicie sesión en la Consola de administración de AWS y abra la consola de IAM.
2. En el panel de navegación de la consola de IAM, elija Roles (Roles). A continuación, seleccione el nombre (no la casilla de verificación) del rol de `AWS ServiceRoleForDocDB-Elastic`.
3. En la página Summary (Resumen) del rol seleccionado, elija la pestaña Access Advisor (Acceso a Advisor).

> **Note**
>
> Si no está seguro de si los clústeres elásticos de Amazon DocumentDB utilizan el rol `AWS ServiceRoleForDocDB-Elastic`, puede intentar eliminar el rol para comprobarlo. Si el servicio utiliza la función, se produce un error en la eliminación y puede ver Regiones de AWS dónde se utiliza la función. Si el rol se está utilizando, debe esperar que la sesión finalice para poder eliminarlo. No se puede revocar la sesión de un rol vinculado a servicios. Si desea eliminar el rol `AWS ServiceRoleForDocDB-Elastic`, primero debe eliminar todos sus clústeres.

Eliminación de todos los clústeres

Para eliminar un clúster en la consola de Amazon DocumentDB:

1. Inicie sesión en la Consola de administración de AWS de Amazon DocumentDB y ábrala.
2. En el panel de navegación, seleccione Clusters (Clústeres).
3. Elija el clúster que desea eliminar.
4. En Actions (Acciones), seleccione Delete (Eliminar).
5. Si aparece el mensaje ¿Crear instantánea final?, elija Sí o No.
6. Si eligió Yes (Sí) en el paso anterior, en Final snapshot name (Nombre de instantánea final) escriba el nombre de la instantánea final.
7. Elija Eliminar.

> **Note**
>
> Puede usar la consola de IAM, la CLI de IAM o la API de IAM para eliminar el rol vinculado a servicios `AWS ServiceRoleForDocDB-Elastic`. Para obtener más información, consulte Eliminación de roles vinculados a servicios en la Guía del usuario de la gestión de identidades y accesos de AWS .

Monitorización de Amazon DocumentDB

La supervisión de sus AWS servicios es una parte importante para mantener sus sistemas en buen estado y funcionando de manera óptima. Es aconsejable recopilar datos de monitorización de todas las partes de su solución de AWS para que le resulte más sencillo depurar y solucionar los errores o la reducción del rendimiento, en caso de que ocurran. Antes de comenzar a monitorizar sus soluciones de AWS , le recomendamos que se plantee las siguientes preguntas:

- ¿Cuáles son los objetivos de la supervisión?
- ¿Qué recursos va a monitorizar?
- ¿Con qué frecuencia va a monitorizar estos recursos?
- ¿Qué herramientas de supervisión va a utilizar?
- ¿Quién es el responsable de realizar el seguimiento?
- ¿A quién se va a notificar y qué ocurre si algo va mal?

Para comprender los patrones de rendimiento actual, identificar las anomalías de rendimiento y elaborar métodos para la resolución de problemas, debe establecer métricas de rendimiento de referencia para distintos momentos y bajo diferentes condiciones de carga. A medida que monitorice su solución de AWS , le recomendamos que guarde los datos de monitorización históricos como referencia futura y para establecer sus métricas de referencia.

En general, los valores aceptables para las métricas de desempeño dependen del aspecto de la referencia y de lo que hace la aplicación. Investigue las variaciones coherentes o de las tendencias con respecto a la referencia. A continuación, se ofrecen algunas sugerencias sobre tipos concretos de métricas:

- Consumo elevado de CPU o RAM: unos valores elevados de consumo de CPU o RAM pueden ser adecuados si se ajustan a los objetivos de su aplicación (de rendimiento o simultaneidad, por ejemplo) y son los esperados.
- Consumo de volumen de almacenamiento: investigue el consumo de almacenamiento (`VolumeBytesUsed`) si el espacio utilizado está por sistema alrededor o por encima del 85 % del espacio del volumen de almacenamiento. Determine si es posible eliminar datos del volumen de almacenamiento o archivar los datos en un sistema diferente para liberar espacio. Para obtener más información, consulte Almacenamiento de Amazon DocumentDB y Cuotas y límites de Amazon DocumentDB.

- Tráfico de red: para el tráfico de red, hable con el administrador de su sistema para saber cuál es el rendimiento esperado para la red de su dominio y para su conexión a Internet. Investigue el tráfico de red si el rendimiento es por sistema inferior al esperado.
- Conexiones a bases de datos: valore la posibilidad de restringir las conexiones a las bases de datos si ve que hay un alto número de conexiones de usuarios junto con una reducción en el rendimiento y el tiempo de respuesta de la instancia. El mejor número de conexiones de usuarios para su instancia variará en función de la clase de instancia y de la complejidad de las operaciones que se estén llevando a cabo.
- Métricas de IOPS: los valores esperados para las métricas de IOPS dependen de la especificación del disco y la configuración del servidor, así que debe usar su referencia para conocer los valores típicos. Investigue si los valores son por sistema diferentes de los valores de referencia. Para un rendimiento óptimo de IOPS, asegúrese de que el conjunto de trabajo típico se ajuste a la memoria para minimizar las operaciones de lectura y escritura.

Amazon DocumentDB (compatible con MongoDB) proporciona una variedad de CloudWatch métricas de Amazon que puede supervisar para determinar el estado y el rendimiento de sus instancias y clústeres de Amazon DocumentDB. Puede ver las métricas de Amazon DocumentDB mediante diversas herramientas, como la consola Amazon DocumentDB AWS CLI CloudWatch , la API y Performance Insights.

Temas

- Supervisión del estado de un clúster de Amazon DocumentDB
- Supervisión del estado de un clúster de Amazon DocumentDB
- Visualización de recomendaciones de Amazon DocumentDB
- Uso de suscripciones a eventos de Amazon DocumentDB
- Supervisión de Amazon DocumentDB con CloudWatch
- Registro de llamadas a la API de Amazon DocumentDB con AWS CloudTrail
- Creación de perfiles de operaciones en Amazon DocumentDB
- Supervisión con información sobre rendimiento

Supervisión del estado de un clúster de Amazon DocumentDB

El estado de un clúster indica la situación de este. Puede ver el estado de un clúster mediante la consola de Amazon DocumentDB o el AWS CLI `describe-db-clusters` comando.

Temas

- Valores de estado del clúster
- Monitorización del estado de un clúster

Valores de estado del clúster

En la siguiente tabla se muestran los valores válidos para el estado de un clúster.

Estado del clúster	Description (Descripción)
`active`	El clúster está activo. Este estado se aplica únicamente a los clústeres elásticos.
`available`	El clúster funciona correctam ente y está disponible. Este estado solo se aplica a clústeres basados en instancia s.
`backing-up`	Se está creando una copia de seguridad del clúster.
`creating`	El clúster se está creando. No se puede obtener acceso a él mientras se está creando.
`deleting`	El clúster se está eliminando. No se puede obtener acceso a él mientras se está eliminando.
`failing-over`	Se está realizando una conmutación por error de la instancia principal a una réplica de Amazon DocumentDB.

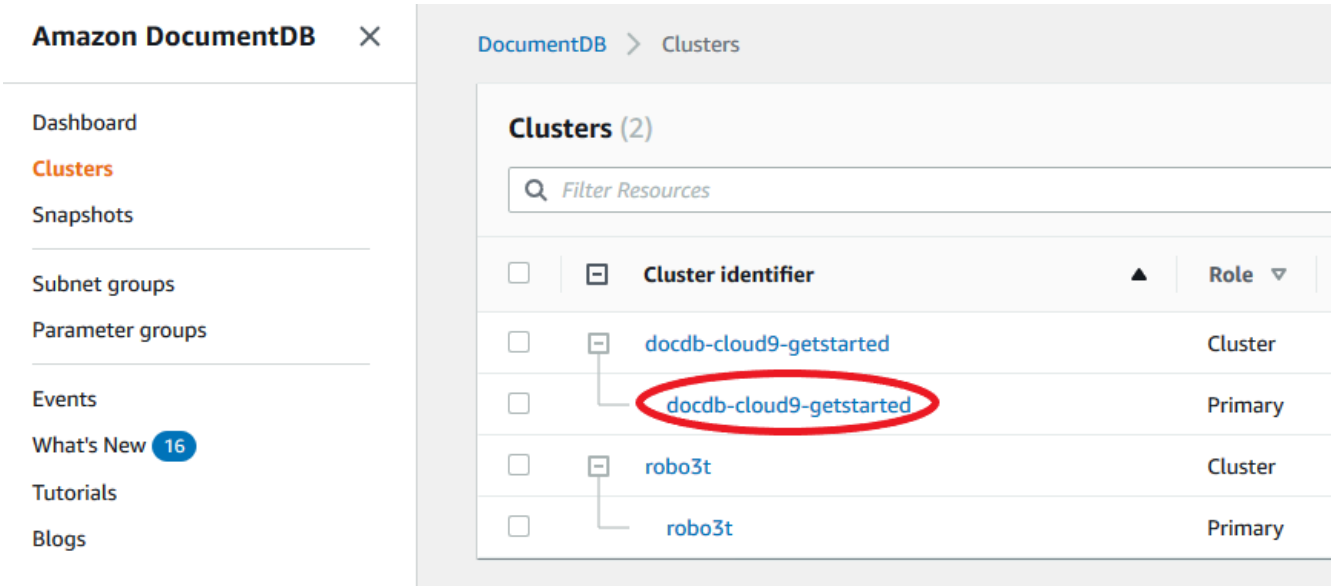
Estado del clúster	Description (Descripción)
`inaccessible-encryption-credentials`	No se puede acceder a la AWS KMS clave utilizada para cifrar o descifrar el clúster.
`maintenance`	Se está aplicando una actualización de mantenimi ento al clúster. Este estado se usa para el mantenimiento de nivel de clúster que Amazon DocumentDB programa con mucha antelación.
`migrating`	Se está restaurando una instantánea de clúster en un clúster.
`migration-failed`	Una migración no se ha realizado correctamente.
`modifying`	El clúster se está modificando porque un cliente ha solicitado su modificación.
`renaming`	El nombre del clúster se está cambiando porque un cliente lo ha solicitado.
`resetting-master-credentials`	Las credenciales maestras del clúster se están restableciendo porque un cliente lo ha solicitad o.
`upgrading`	Se está actualizando la versión del motor del clúster.

Monitorización del estado de un clúster

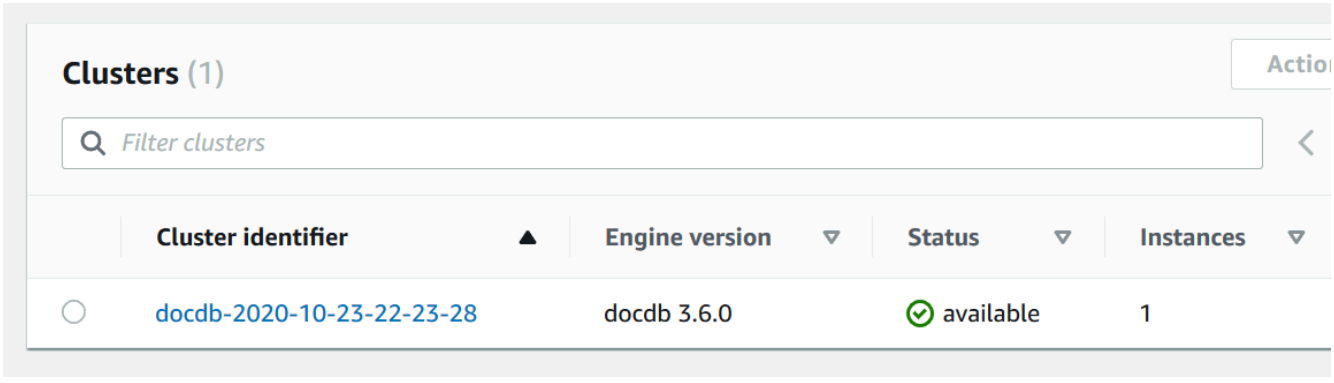
Using the Consola de administración de AWS

Cuando utilice el Consola de administración de AWS para determinar el estado de un clúster, utilice el siguiente procedimiento.

1. Inicie sesión en y abra la Consola de administración de AWS consola de Amazon DocumentDB en https://console.aws.amazon.com /docdb.
2. En el panel de navegación, seleccione Clusters (Clústeres).
3. En el cuadro de navegación de clústeres, verá la columna Identificador del clúster. Las instancias se muestran en clústeres, de forma similar a la siguiente captura de pantalla.



4. En la columna Identificador de clúster, busque el nombre de la instancia que le interese. A continuación, para encontrar el estado de la instancia, consulte en esa fila la columna Estado, tal y como se muestra a continuación.



Using the AWS CLI

Cuando utilice el AWS CLI para determinar el estado de un clúster, utilice la operación. `describe-db-clusters` El siguiente código busca el estado del clúster `sample-cluster`.

Para Linux, macOS o Unix:

```
aws docdb describe-db-clusters \
    --db-cluster-identifier sample-cluster  \
    --query 'DBClusters[*].[DBClusterIdentifier,Status]'
```

Para Windows:

```
aws docdb describe-db-clusters ^
    --db-cluster-identifier sample-cluster  ^
    --query 'DBClusters[*].[DBClusterIdentifier,Status]'
```

La salida de esta operación será similar a lo que se indica a continuación.

```
[
    [
        "sample-cluster",
        "available"
    ]
]
```

Supervisión del estado de un clúster de Amazon DocumentDB

Amazon DocumentDB proporciona información sobre el estado actual de cada instancia configurada de la base de datos.

Hay tres tipos de estado que puede ver para una instancia de Amazon DocumentDB:

- Estado de la instancia: este estado se muestra en la columna Estado de la tabla de clústeres Consola de administración de AWS y muestra el estado actual del ciclo de vida de la instancia. Los valores que se muestran en la columna Estado se derivan del campo `Status` de la respuesta de la API de `DescribeDBCluster`.
- Estado de estado de la instancia: este estado se muestra en la columna de estado de la instancia de la tabla de clústeres de la Consola de administración de AWS y muestra si el motor de base de

datos, el componente responsable de administrar y recuperar los datos, está en funcionamiento. Los valores que se muestran en la columna Estado de la instancia se basan en la métrica CloudWatch `EngineUptime` del sistema Amazon.

- Estado de mantenimiento: este estado se muestra en la columna Mantenimiento de la tabla de clústeres Consola de administración de AWS e indica el estado de cualquier evento de mantenimiento que deba aplicarse a una instancia. El estado de mantenimiento es independiente del estado de las demás instancias y se deriva de la API de `PendingMaintenanceAction`. Para obtener más información sobre el estado del mantenimiento, consulte Mantenimiento de Amazon DocumentDB.

Temas

- Valores de estado de instancia
- Monitorear el estado de la instancia mediante Consola de administración de AWS o AWS CLI
- Estado de una instancia
- Supervisar el estado de la instancia mediante el Consola de administración de AWS

Valores de estado de instancia

En la siguiente tabla se muestran los posibles valores de estado de las instancias y cómo se factura para cada estado. Muestra si se le facturará la instancia y el almacenamiento, solo el almacenamiento o si no se le facturará. Para todos los estados de instancia, se le factura siempre el uso de copia de seguridad.

estado de instancias	Facturado	Description (Descripción)
`available`	Facturado	La instancia funciona correctamente y está disponible.
`backing-up`	Facturado	Se está creando una copia de seguridad de la instancia.
`configuring-log-exports`	Facturado	La publicación de archivos de registro en Amazon CloudWatch Logs está habilitada o deshabilitada en esta instancia.

estado de instancias	Facturado	Description (Descripción)
`creating`	No facturado	La instancia se está creando. No se puede obtener acceso a la instancia mientras se está creando.
`deleting`	No facturado	La instancia se está eliminando.
`failed`	No facturado	La instancia ha generado un error y Amazon DocumentDB no ha podido recuperarla. Para recuperar los datos, realice una point-in-time restauración a la última hora de restauración de la instancia.
`inaccessible-encryption-credentials`	No facturado	No se pudo acceder a la AWS KMS clave que se usa para cifrar o descifrar la instancia.
`incompatible-network`	No facturado	Amazon DocumentDB está intentando realizar una acción de recuperación en una instancia, pero no puede hacerlo porque la VPC está en un estado que impide completar la acción. Este estado puede darse si, por ejemplo, todas las direcciones IP disponibles en una subred estaban en uso y Amazon DocumentDB no puede obtener una dirección IP para la instancia.
`maintenance`	Facturado	Amazon DocumentDB está aplicando una actualización de mantenimiento a la instancia. Este estado se usa para el mantenimiento de nivel de instancia que Amazon DocumentDB programa con mucha antelación. Estamos evaluando formas de exponer otras acciones de mantenimiento a los clientes a través de este estado.

estado de instancias	Facturado	Description (Descripción)
`modifying`	Facturado	La instancia se está modificando debido a una solicitud para modificar la instancia.
`rebooting`	Facturado	La instancia se está reiniciando debido a una solicitud o un proceso de Amazon DocumentDB que requiere el reinicio de la instancia.
`renaming`	Facturado	El nombre de la instancia se está cambiando debido a una solicitud de cambio de nombre.
`resetting-master-credentials`	Facturado	Las credenciales maestras de la instancia se están restableciendo debido a una solicitud de restablecimiento.
`restore-error`	Facturado	La instancia detectó un error al intentar realizar la restauración en una instantánea point-in-time o desde ella.
`starting`	Facturado para almacenamiento	La instancia se está iniciando.
`stopped`	Facturado para almacenamiento	La instancia se ha detenido.
`stopping`	Facturado para almacenamiento	La instancia se está deteniendo.

estado de instancias	Facturado	Description (Descripción)
`storage-full`	Facturado	La instancia ha alcanzado su asignació n de capacidad de almacenamiento. Es un estado crítico y se debe corregir de inmediato. Aumente el almacenam iento modificando la instancia. Configura CloudWatch las alarmas de Amazon para que te avisen cuando el espacio de almacenamiento se esté agotando para que no te encuentres con esta situación.

Monitorear el estado de la instancia mediante Consola de administración de AWS o AWS CLI

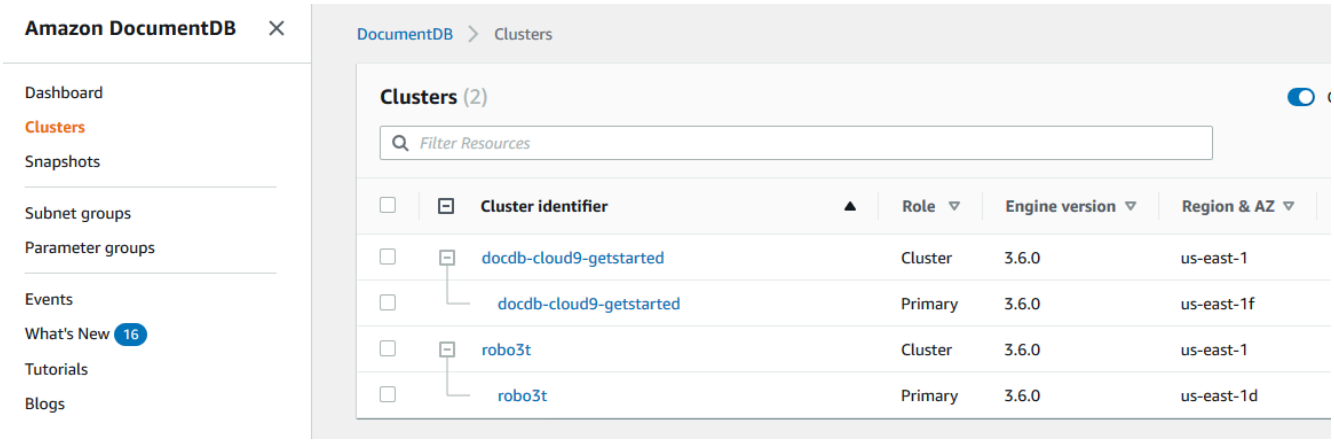
Usa Consola de administración de AWS o AWS CLI para monitorear el estado de tu instancia.

Using the Consola de administración de AWS

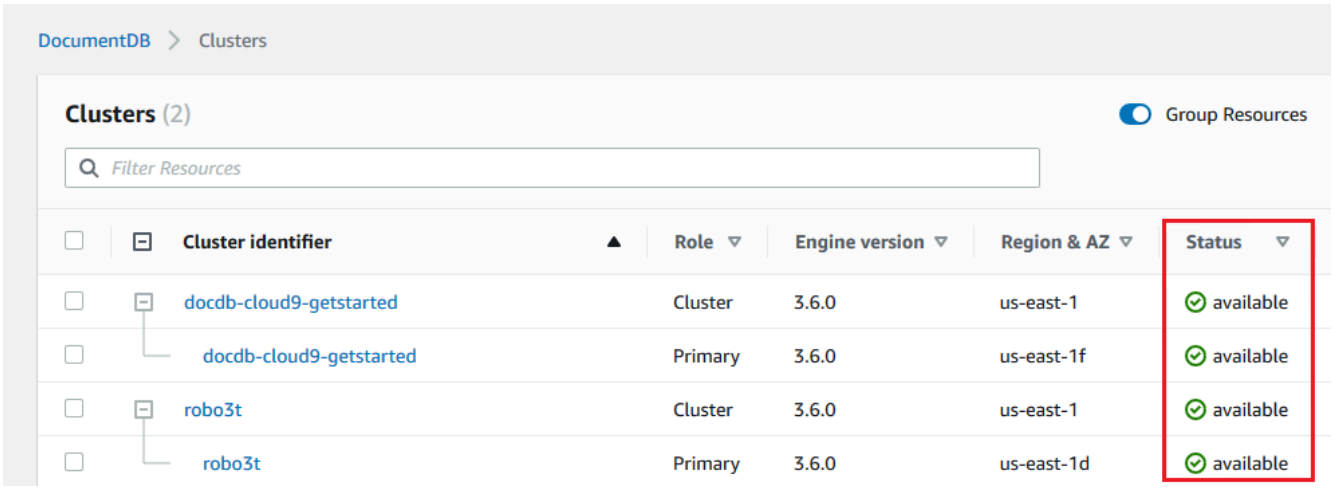
Cuando utilice el Consola de administración de AWS para determinar el estado de un clúster, utilice el siguiente procedimiento.

1. Inicie sesión en y abra la Consola de administración de AWS consola de Amazon DocumentDB en https://console.aws.amazon.com /docdb.
2. En el panel de navegación, seleccione Clusters (Clústeres).

> **Note**
>
> Tenga en cuenta que en el cuadro de navegación de clústeres, la columna Identificador de clústeres muestra tanto los clústeres como las instancias. Las instancias se muestran en clústeres, de forma similar a la siguiente captura de pantalla.



3. Busque el nombre de la instancia que le interesa. A continuación, para encontrar el estado de la instancia, consulte en esa fila la columna Status (Estado), tal y como se muestra a continuación.



Using the AWS CLI

Cuando utilice el AWS CLI para determinar el estado de un clúster, utilice la operación. `describe-db-instances` El siguiente código muestra el estado de la instancia `sample-cluster-instance-01`.

Para Linux, macOS o Unix:

```
aws docdb describe-db-instances \
          --db-instance-identifier sample-cluster-instance-01  \
          --query 'DBInstances[*].[DBInstanceIdentifier,DBInstanceStatus]'
```

Para Windows:

```
aws docdb describe-db-instances ^
          --db-instance-identifier sample-cluster-instance-01  ^
          --query 'DBInstances[*].[DBInstanceIdentifier,DBInstanceStatus]'
```

La salida de esta operación será similar a lo que se indica a continuación.

```
[
          [
              "sample-cluster-instance-01",
              "available"
          ]
      ]
```

Estado de una instancia

Encuentre los valores de estado posibles para instancias de base de datos en la siguiente tabla. La columna de estado de la instancia, ubicada en la tabla de clústeres del Consola de administración de AWS, muestra si el motor de base de datos, el componente responsable de almacenar, administrar y recuperar los datos, funciona con normalidad. Esta columna también indica si la métrica `EngineUptime` del sistema, disponible en CloudWatch, muestra el estado de cada instancia.

Estado de una instancia	Description (Descripción)
buen estado	El motor de base de datos se ejecuta en la instancia de Amazon DocumentDB.
Mal estado	El motor de base de datos no se está ejecutando o se reinició hace menos de un minuto.

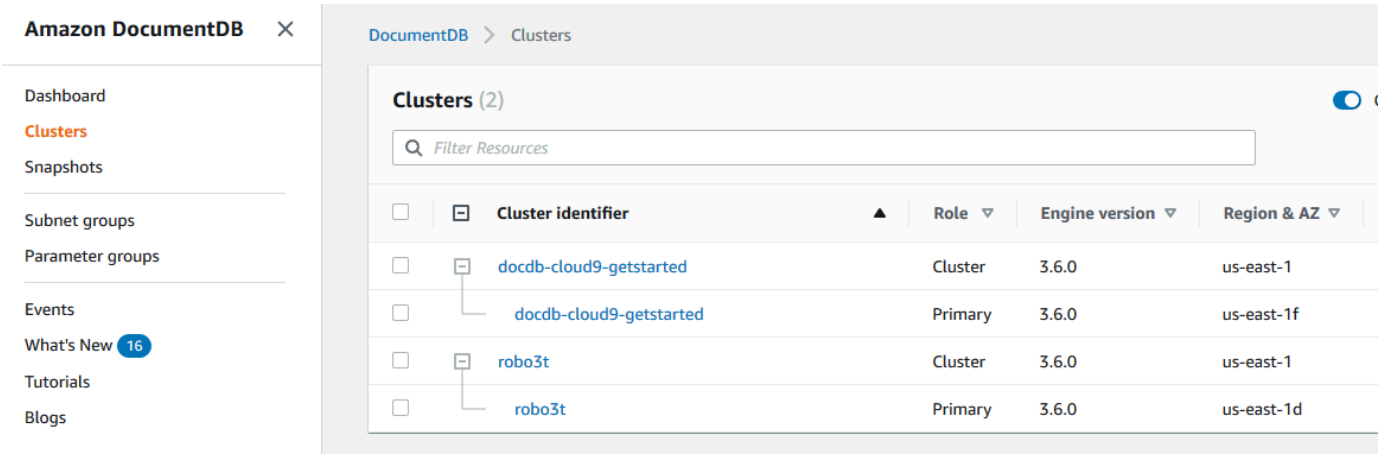
Supervisar el estado de la instancia mediante el Consola de administración de AWS

Utilice el Consola de administración de AWS para supervisar el estado de salud de la instancia.

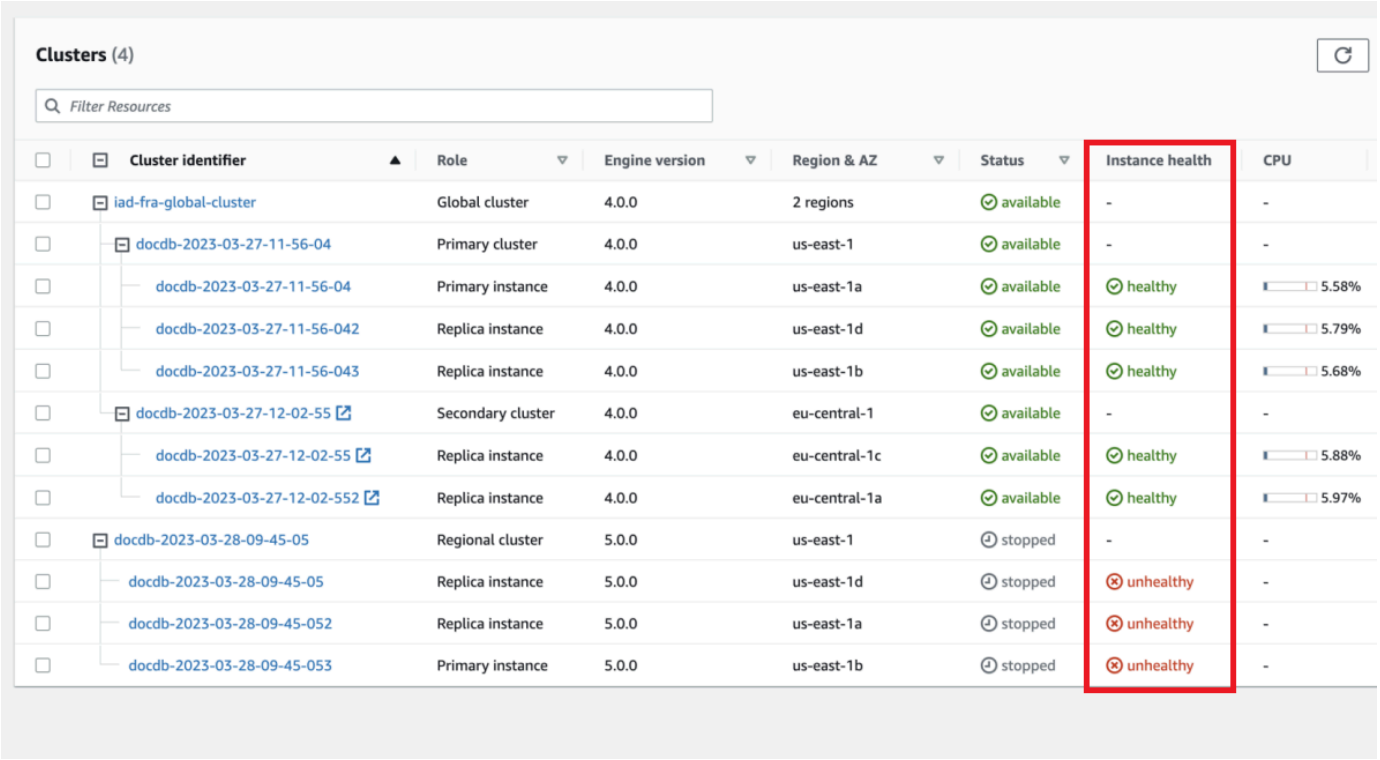
Cuando la utilices Consola de administración de AWS, sigue los siguientes pasos para entender el estado de salud de la instancia.

1. Inicie sesión en y abra la Consola de administración de AWS consola de Amazon DocumentDB en https://console.aws.amazon.com /docdb.
2. En el panel de navegación, seleccione Clusters (Clústeres).

> **Note**
>
> Tenga en cuenta que en el cuadro de navegación Clústeres, la columna Identificador del clúster muestra tanto los clústeres como las instancias. Las instancias se muestran en clústeres, de forma similar a la siguiente captura de pantalla.



3. Busque el nombre de la instancia que le interesa. A continuación, para encontrar el estado de la instancia, consulte en esa fila la columna Estado, tal y como se muestra a continuación:



> **Note**
>
> El sondeo del estado de las instancias se realiza cada 60 segundos y se basa en la métrica del CloudWatch `EngineUptime` sistema. Los valores de la columna Estado de la instancia se actualizan automáticamente.

Visualización de recomendaciones de Amazon DocumentDB

Amazon DocumentDB proporciona una lista de recomendaciones automatizadas para recursos de base de datos, como instancias y clústeres. Estas recomendaciones proporcionan instrucciones de las prácticas recomendadas analizando los datos de rendimiento, el uso y la configuración de la instancia y clúster.

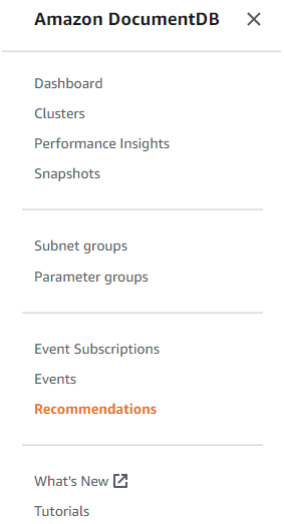
Para ver ejemplos de estas recomendaciones, consulte lo siguiente:

Tipo	Descripción	Recomendación	Información adicional
Una instancia	El clúster solo contiene una instancia	Rendimiento y disponibilidad: recomendamos añadir otra instancia con la misma clase de instancia en una zona de disponibilidad diferente.	Alta disponibilidad y replicación de Amazon DocumentDB

Amazon DocumentDB genera recomendaciones para un recurso cuando se crea o modifica el recurso. Amazon DocumentDB analiza también periódicamente sus recursos y genera recomendaciones.

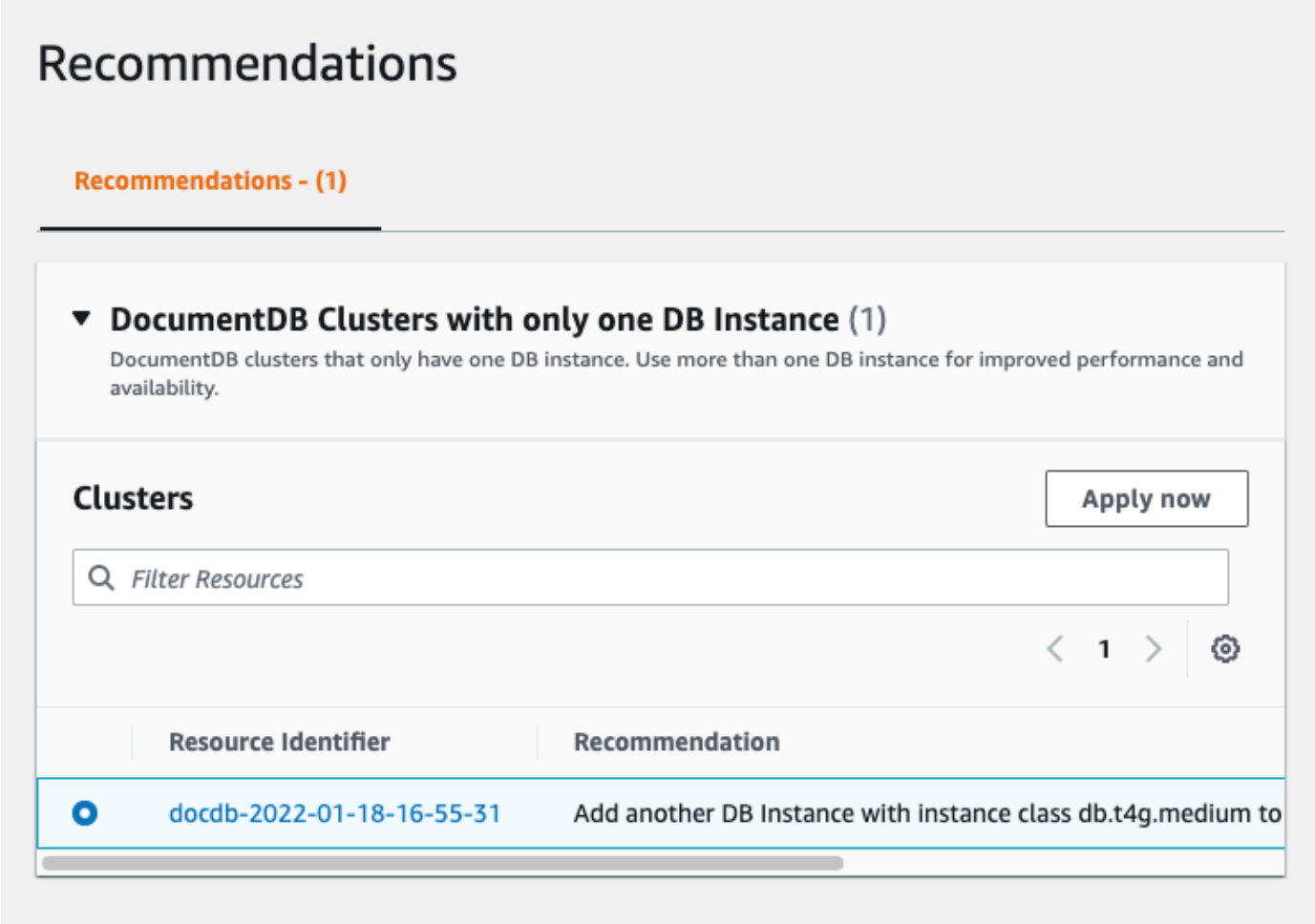
Visualización de las recomendaciones de Amazon DocumentDB y toma de medidas al respecto

1. Inicie sesión en y abra la Consola de administración de AWS consola de Amazon DocumentDB en https://console.aws.amazon.com /docdb.
2. En el panel de navegación, seleccione Recomendaciones:



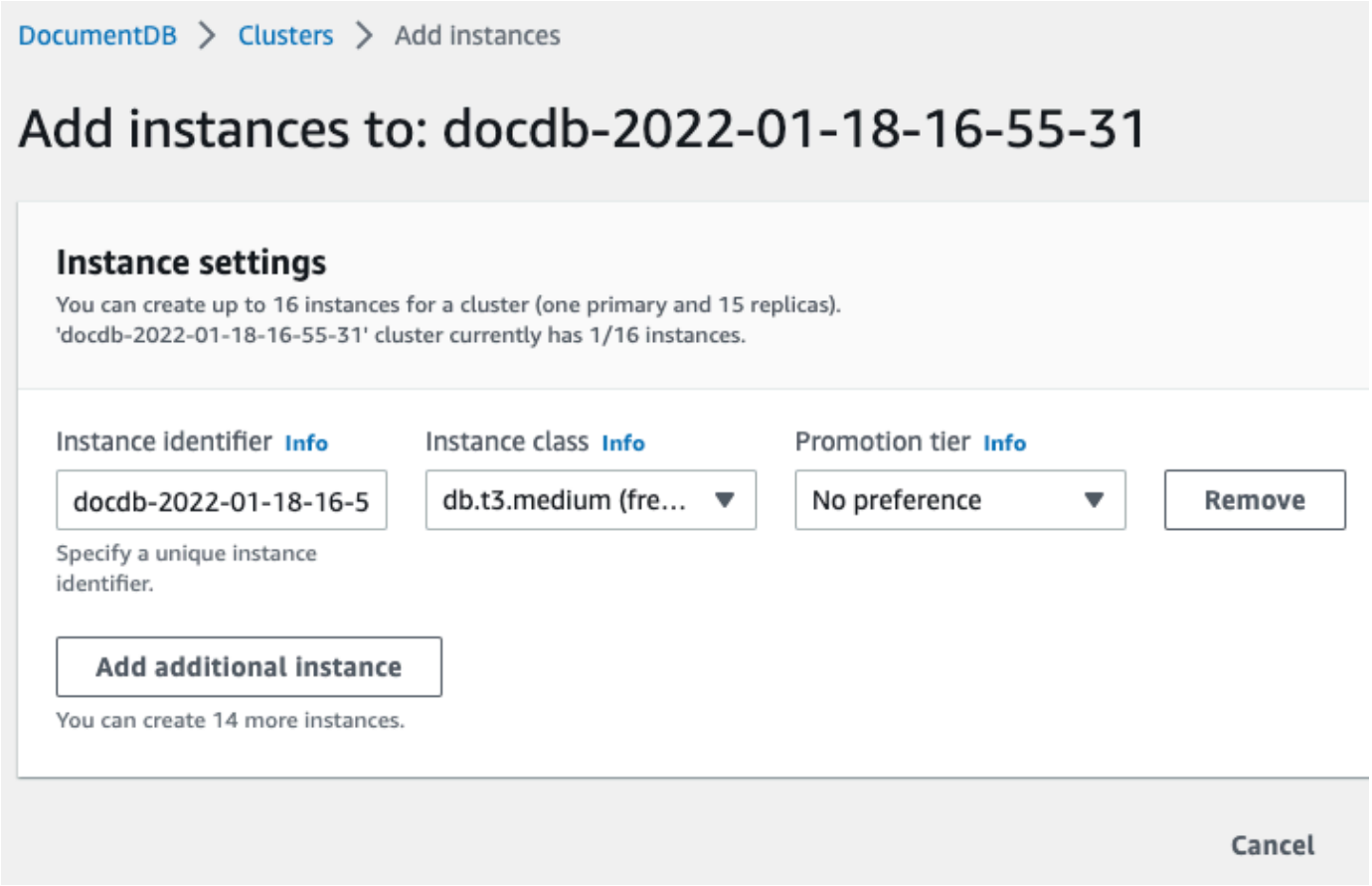
3. En el cuadro de diálogo Recomendaciones, amplíe la sección de interés y seleccione la tarea recomendada.

En el siguiente ejemplo, la tarea recomendada se aplica a un clúster de Amazon DocumentDB con una sola instancia. La recomendación es añadir otra instancia para mejorar el rendimiento y la disponibilidad.



4. Haga clic en Aplicar ahora.

   En este ejemplo, aparece el cuadro de diálogo Agregar instancias:



5. Modifique la configuración de la nueva instancia y haga clic en Crear.

Uso de suscripciones a eventos de Amazon DocumentDB

Amazon RDS utiliza Amazon Simple Notification Service (Amazon SNS) para proporcionar notificaciones cuando se produce un evento de Amazon DocumentDB. Estas notificaciones pueden realizarse con cualquier método que admita Amazon SNS para una Región de AWS, como un email, un mensaje de texto o una llamada a un punto de conexión HTTP.

Amazon DocumentDB agrupa estos eventos en categorías a las que puede suscribirse para recibir una notificación cada vez que se produzca un evento en esa categoría. Puede suscribirse a una categoría de eventos para una instancia, un clúster, una instantánea, una instantánea de clúster, o para un grupo de parámetros. Por ejemplo, si se suscribe a la categoría Backup de una instancia determinada, recibe una notificación cada vez que se produzca un evento relacionado con las copias de seguridad que afecte a dicha instancia. También recibirá una notificación cuando cambie una suscripción de eventos.

Los eventos se producen en el clúster y en el nivel de instancia, por lo que puede recibir eventos si se suscribe a un clúster o a una instancia.

Las suscripciones de eventos se envían a las direcciones que se proporcionan al crear la suscripción. Es posible que le interese crear distintas suscripciones como, por ejemplo, una que reciba todas las notificaciones de eventos y otra que incluya únicamente los eventos críticos para las instancias de producción. Puede desactivar fácilmente las notificaciones sin eliminar una suscripción. Para ello, defina el botón de opción Activado en No en la consola de Amazon DocumentDB.

> **Important**
>
> Amazon DocumentDB no garantiza el orden de los eventos enviados en una secuencia de eventos. El orden de los eventos está sujeto a cambio.

Amazon DocumentDB utiliza el nombre de recurso de Amazon (ARN) de un tema de Amazon SNS para identificar cada suscripción. La consola de Amazon DocumentDB crea el ARN automáticamente cuando se crea la suscripción.

La facturación de las suscripciones a eventos de Amazon DocumentDB se realiza a través de Amazon SNS. Se aplican las tarifas de Amazon SNS cuando se utiliza la notificación de eventos. Para obtener más información, consulte Amazon Simple Notification Service Pricing. Además de los cargos de Amazon SNS, Amazon DocumentDB no factura las suscripciones a eventos.

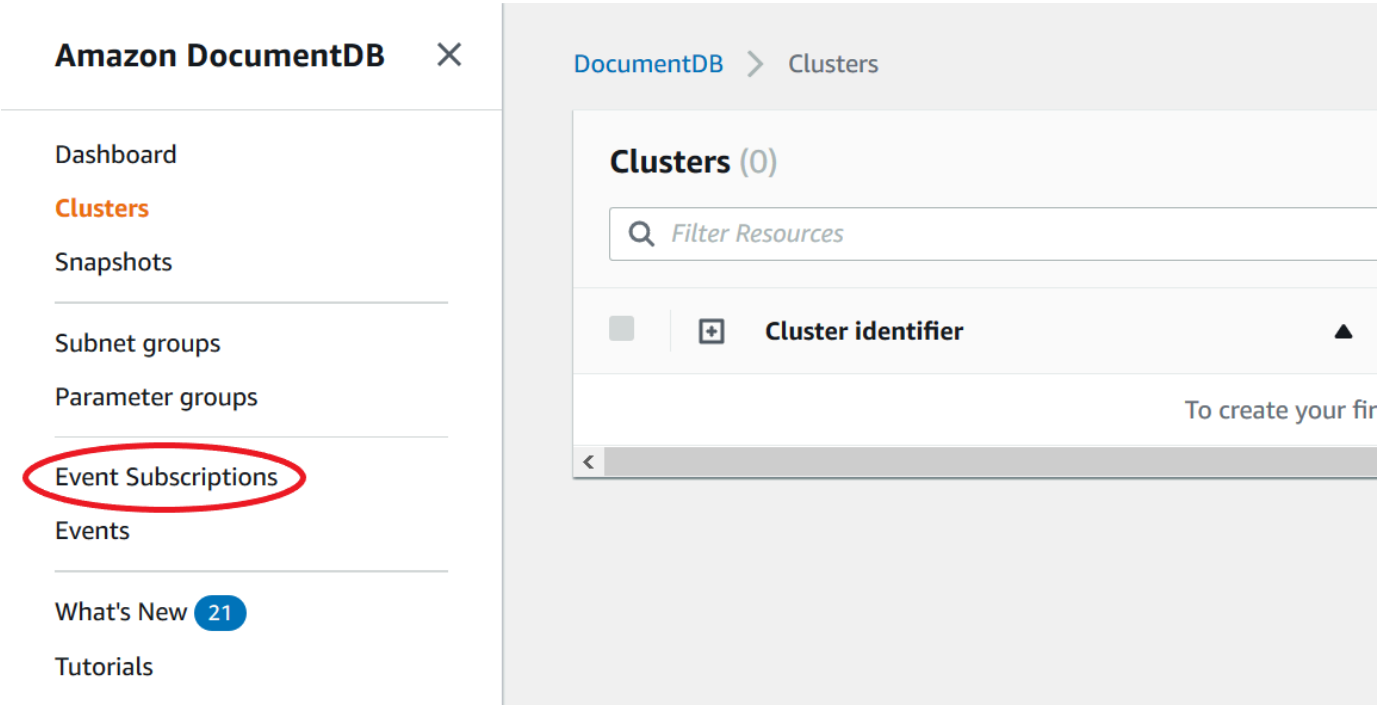
Temas

- Suscripción a eventos de Amazon DocumentDB
- Administración de suscripciones a notificaciones de eventos de Amazon DocumentDB
- Categorías y mensajes de eventos de Amazon DocumentDB

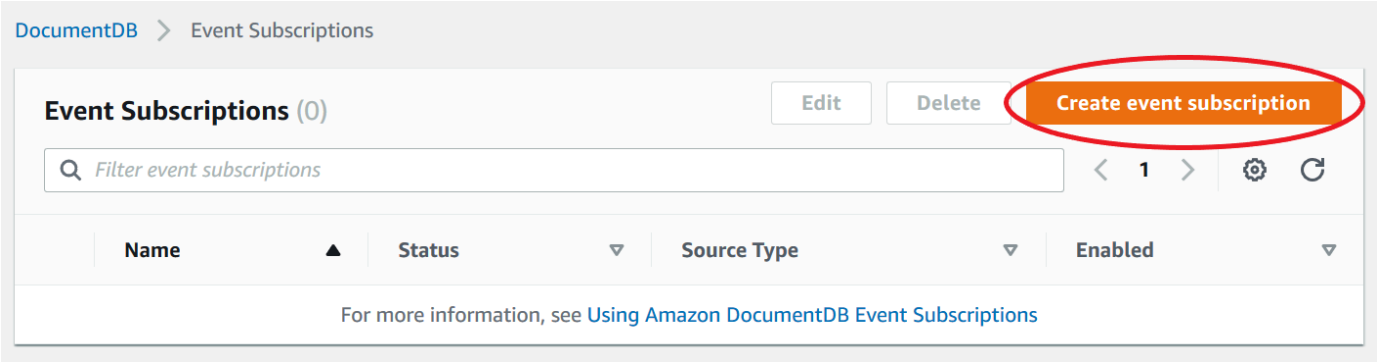
Suscripción a eventos de Amazon DocumentDB

Puede utilizar la consola Amazon DocumentDB para suscribirse a las suscripciones a eventos de la siguiente manera:

1. Inicie sesión en la Consola de administración de AWS en https://console.aws.amazon.com/docdb.
2. En el panel de navegación seleccione Event Subscriptions (Suscripciones de eventos).

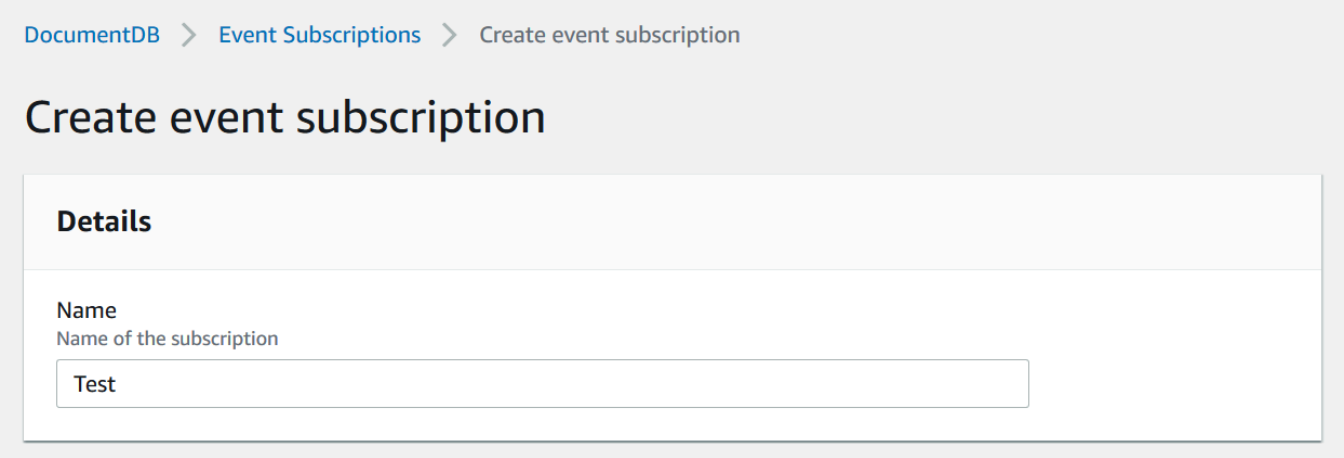


3. En la página Event Subscriptions (Suscripciones de eventos) seleccione Create Event Subscription (Crear suscripción de eventos).

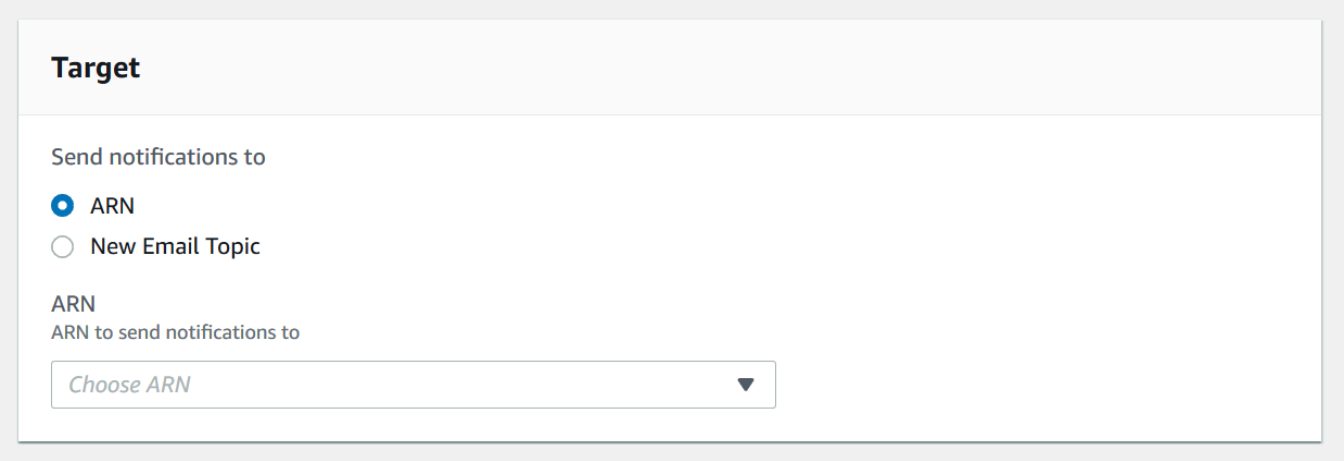


4. En el cuadro de diálogo Create Event Subscription (Crear suscripción de eventos), haga lo siguiente:

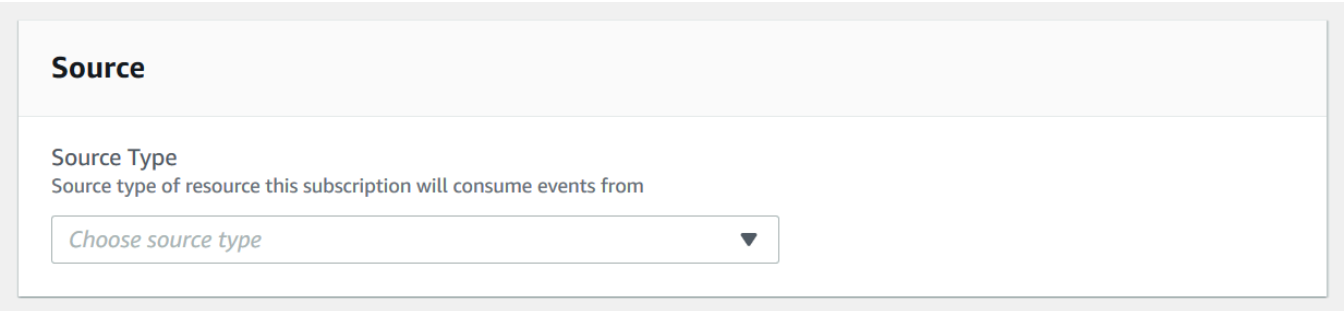
   - En Name (Nombre) escriba un nombre para la suscripción de notificación de evento.



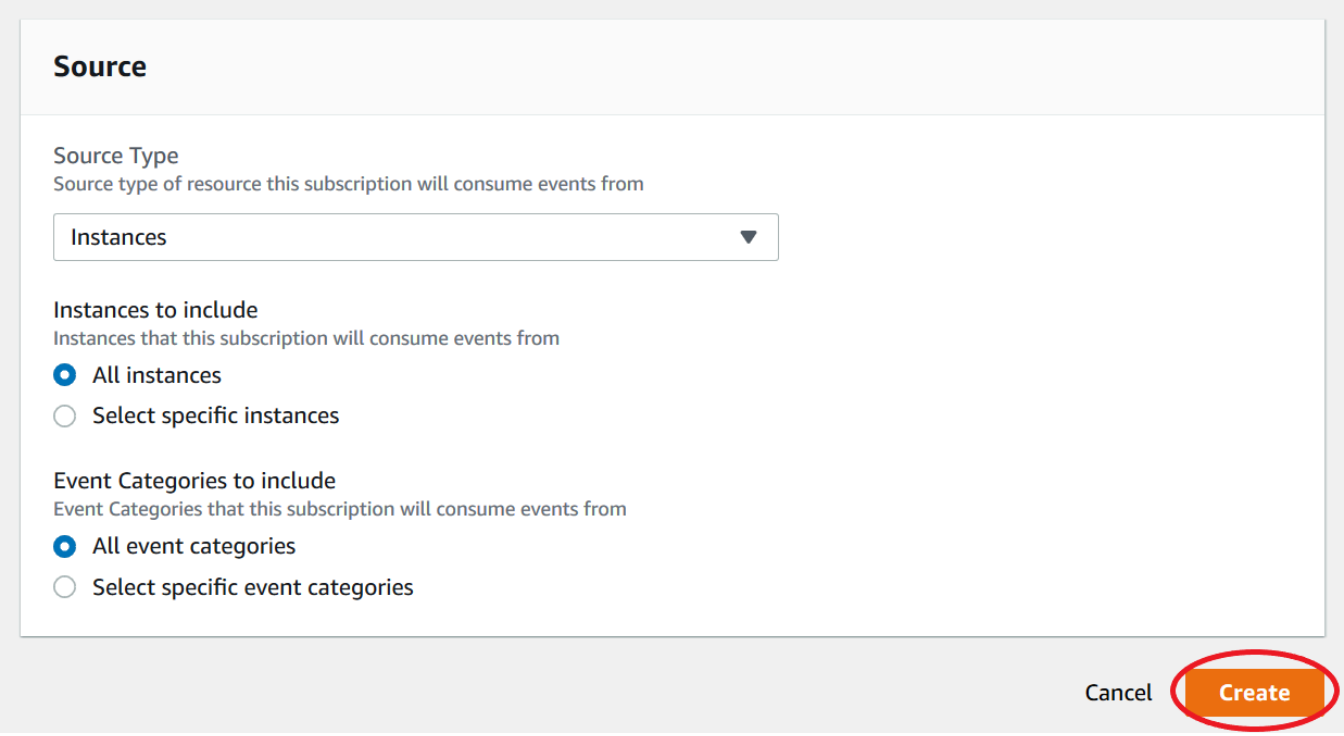
- En Destino, seleccione a dónde quiere enviar las notificaciones. Puede elegir un ARN existente o elegir Nuevo tema de correo electrónico para introducir el nombre de un tema y una lista de destinatarios.



- En Origen elija un tipo de origen. En función del tipo de origen que haya seleccionado, seleccione las categorías y orígenes del evento de las que desea recibir notificaciones.



- Seleccione Crear.

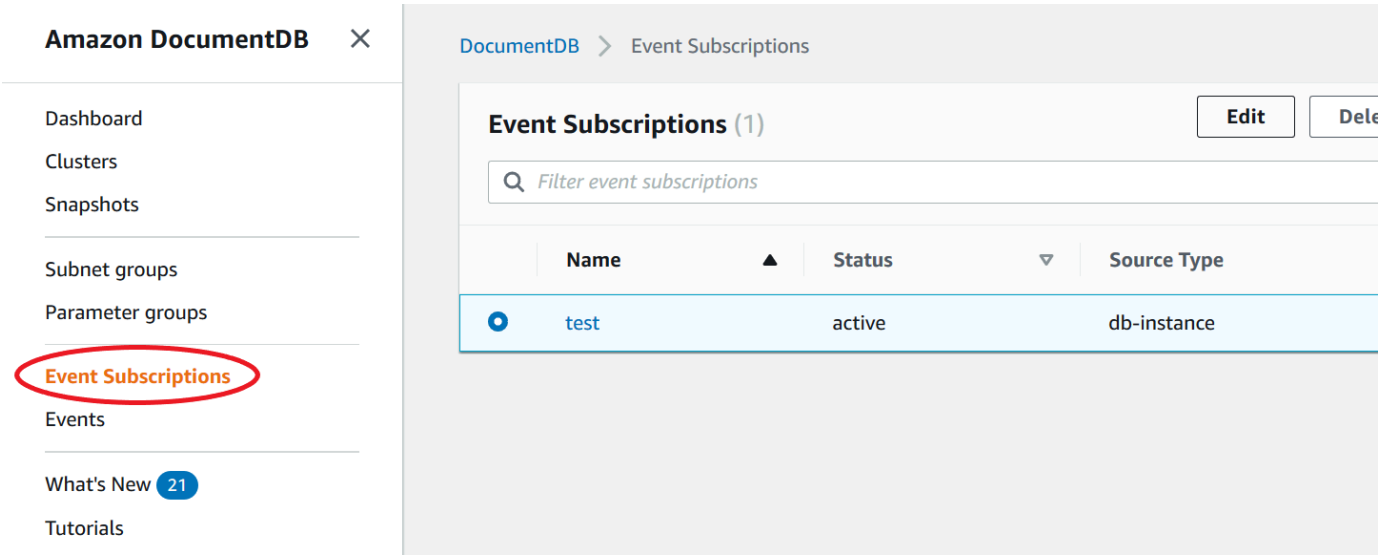


Administración de suscripciones a notificaciones de eventos de Amazon DocumentDB

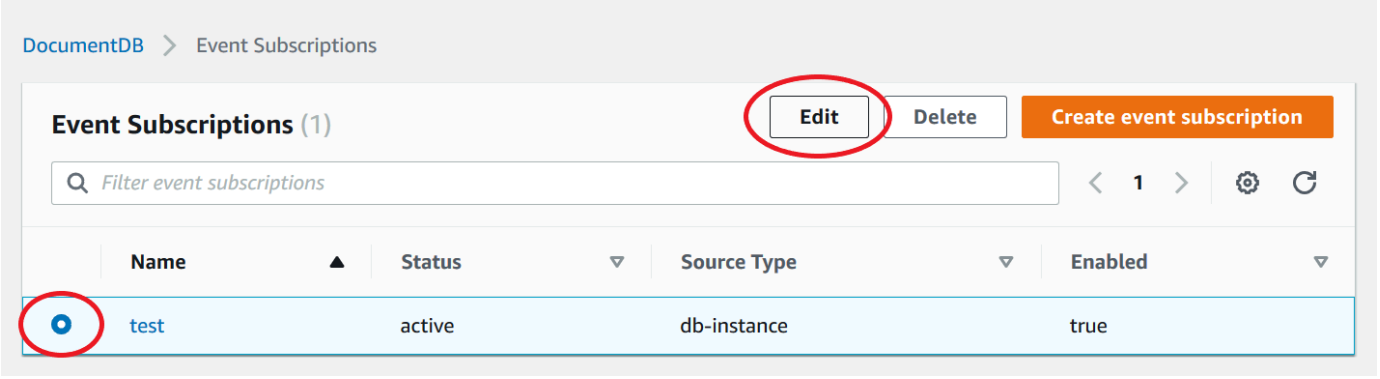
Si selecciona Suscripciones a eventos en el panel de navegación de la consola de Amazon DocumentDB, puede ver las categorías de suscripciones y una lista de sus suscripciones actuales. También puede modificar o eliminar una suscripción específica.

Modificación de sus suscripciones actuales de notificación de eventos de Amazon DocumentDB

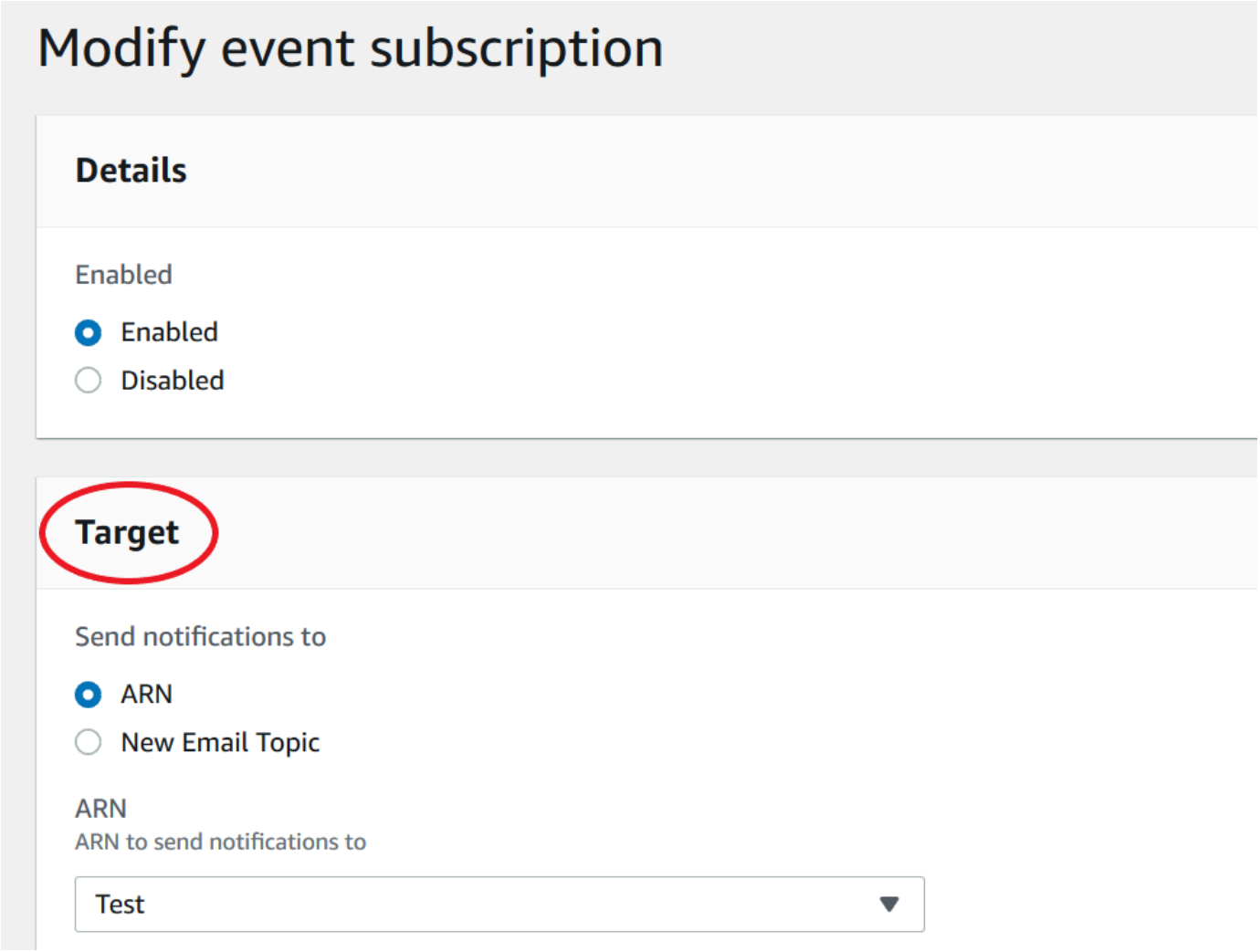
1. Inicie sesión en la Consola de administración de AWS en https://console.aws.amazon.com/docdb.
2. En el panel de navegación seleccione Event Subscriptions (Suscripciones de eventos). El panel Event subscriptions (Suscripciones de eventos) muestra todas sus suscripciones a notificaciones de eventos.



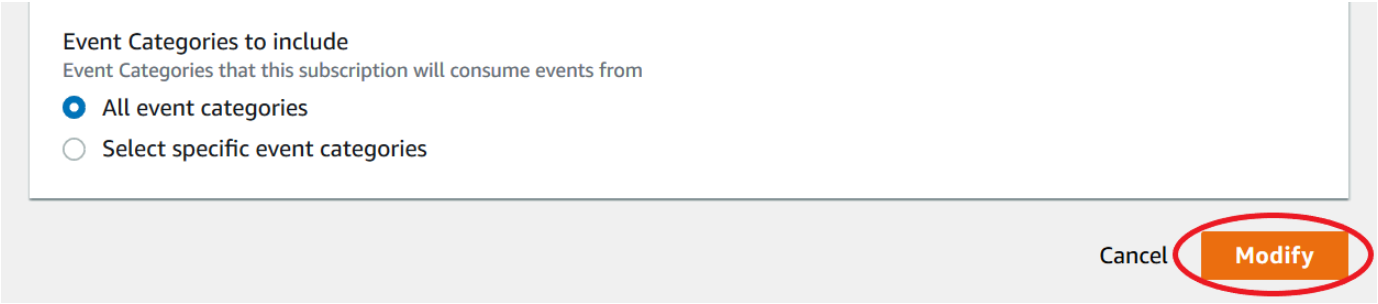
3. En el panel Event subscriptions (Suscripciones de eventos), elija la suscripción que desea modificar y elija Edit (Editar).



4. Realice los cambios que desee en la suscripción en las secciones Target (Objetivo) o Source (Fuente). Puede añadir o eliminar identificadores de origen activándolos o desactivándolos en la sección Origen.



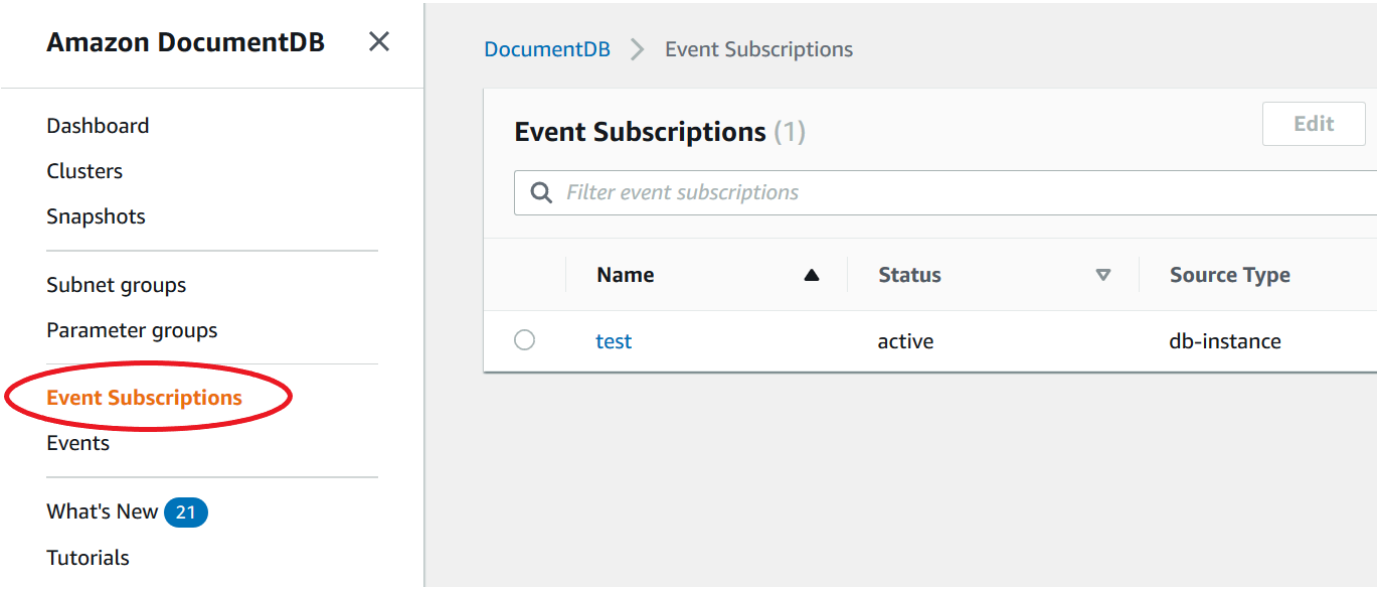
5. Elija Modificar. La consola de Amazon DocumentDB indica que se está modificando la suscripción.



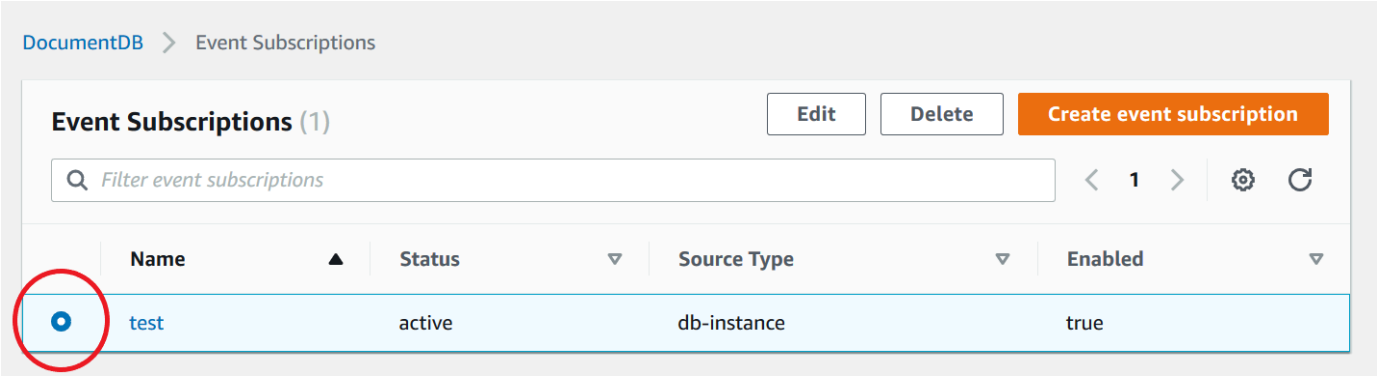
Eliminación de una suscripción de notificación de eventos de Amazon DocumentDB

Puede eliminar una suscripción cuando ya no la necesite. Los suscriptores del tema dejarán de recibir notificaciones de los eventos especificados en la suscripción.

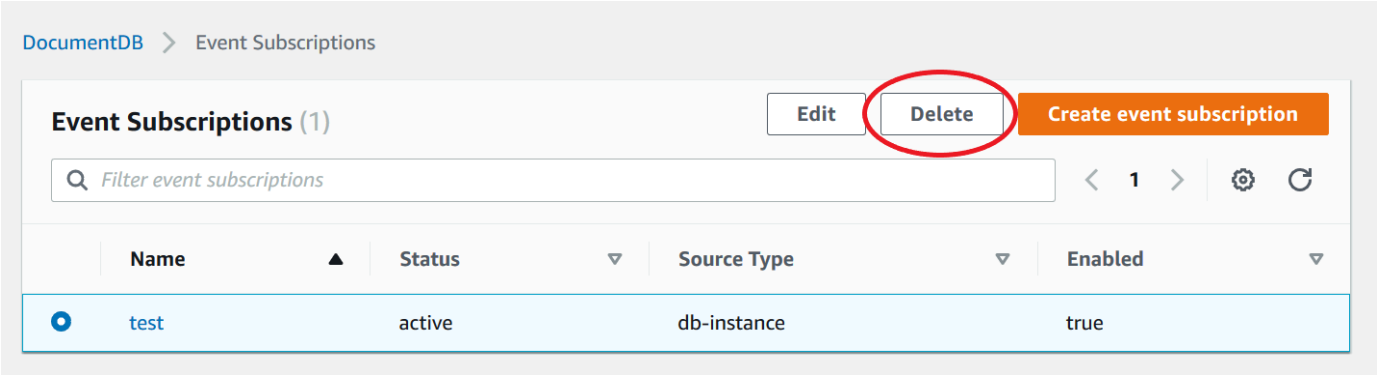
1. Inicie sesión en la Consola de administración de AWS en https://console.aws.amazon.com/docdb.
2. En el panel de navegación seleccione Event Subscriptions (Suscripciones de eventos).



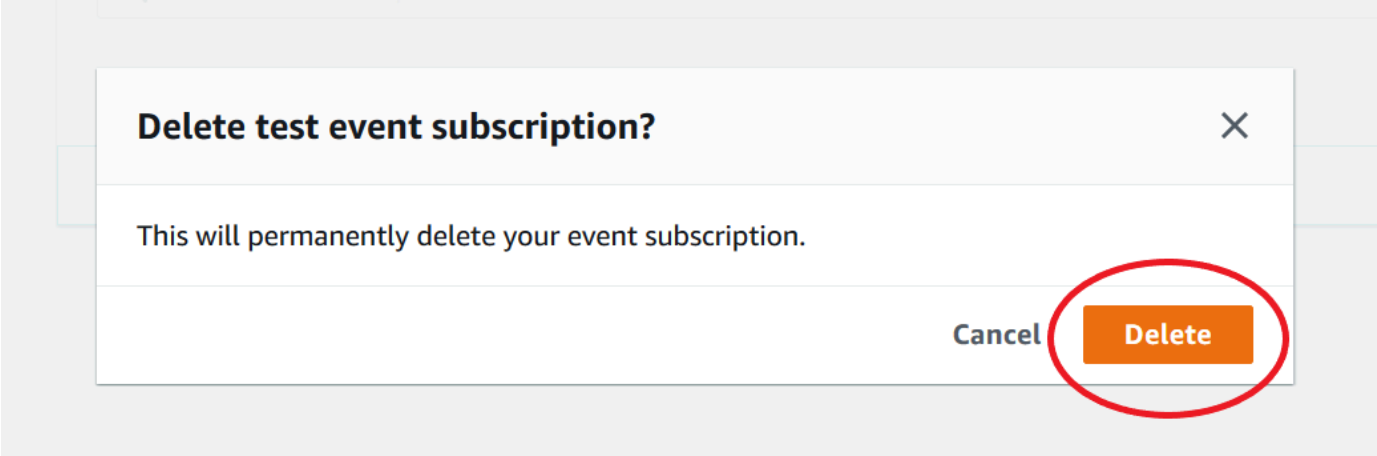
3. En el panel Suscripciones a eventos, seleccione la suscripción que desea eliminar.



4. Elija Eliminar.



5. Aparecerá una ventana emergente en la que se le preguntará si desea eliminar esta notificación de forma permanente. Elija Eliminar.



Categorías y mensajes de eventos de Amazon DocumentDB

Amazon DocumentDB genera un número significativo de eventos en categorías a las que puede suscribirse a través de la consola. Cada categoría se aplica a un tipo de origen, que puede ser una instancia, un clúster, una instantánea o un grupo de parámetros.

> **Note**
>
> Amazon DocumentDB utiliza las definiciones e ID de eventos de Amazon RDS existentes.

Eventos de Amazon DocumentDB que se originan en instancias

Categoría	Descripción
availability	Instancia reiniciada.
disponibilidad	Instancia cerrada.
cambio de configuración	Se está aplicando la modificación a la clase de instancia.
cambio de configuración	Ha finalizado la aplicación de la modificación a una clase de instancia.

Categoría	Descripción
cambio de configuración	Restablezca las credenciales principales.
creación	Instancia creada.
eliminación	Se ha eliminado la instancia
error	Se ha producido un error en la instancia debido a una configuración incompatible o a un problema de almacenamiento subyacente. Comience una restauración a un momento dado para la instancia.
notificación	Se ha detenido la instancia.
notificación	Se ha iniciado la instancia.
notificación	La instancia se está iniciando debido a que se supera el tiempo máximo permitido para estar detenida.
recuperación	Se ha iniciado la recuperación de la instancia. El tiempo de recuperación dependerá de la cantidad de datos que deban recuperarse.
recuperación	Ha finalizado la recuperación de la instancia.
Creación de parches de seguridad	La actualización del sistema operativo está disponible para su instancia. Para obtener más información acerca de cómo se aplican las actualizaciones, consulte Mantenimiento de Amazon DocumentDB.

Eventos de Amazon DocumentDB que se originan en un clúster

Categoría	Descripción
creación	Se ha creado un clúster
eliminación	Se ha eliminado un clúster.
conmutación por error	Volver a promocionar el principal anterior.
conmutación por error	Se ha completado la conmutación por error en la instancia.
conmutación por error	Se ha iniciado la misma conmutación por error de AZ en la instancia de base de datos: %s
conmutación por error	Se ha iniciado la misma conmutación por error de AZ en la instancia de base de datos: %s
conmutación por error	Se ha iniciado la conmutación por error entre AZ en la instancia de base de datos: %s
mantenimiento	Se ha parcheado el clúster.
mantenimiento	El clúster de base de datos tiene un estado que no se puede actualizar: %s
notificación	El clúster se ha detenido.
notificación	El clúster se ha iniciado.
notificación	La detención del clúster ha producido un error.
notificación	El clúster se está iniciando debido a que se supera el tiempo máximo permitido para estar detenida.
notificación	Se ha cambiado el nombre del clúster de %s a %s.

Eventos de Amazon DocumentDB que se originan en una instantánea de clúster

En la siguiente tabla se muestra la categoría de eventos y una lista de los eventos que pueden producirse cuando el tipo de origen es una instantánea de clúster de Amazon DocumentDB.

Categoría	Descripción
copia de seguridad	Crear una instantánea manual del clúster.
copia de seguridad	Se ha creado una instantánea manual del clúster.
copia de seguridad	Creación de instantáneas de clúster automatizadas.
copia de seguridad	Se ha creado una instantánea de clúster automatizada.

Eventos de Amazon DocumentDB que se originan en un grupo de parámetros

En la siguiente tabla, se muestra la categoría de eventos y una lista de eventos correspondiente a un grupo de parámetros como tipo de origen.

Categoría	Descripción
cambio de configuración	Se actualizó el parámetro %s a %s con el método de aplicación %s

Supervisión de Amazon DocumentDB con CloudWatch

Amazon DocumentDB (compatible con MongoDB) se integra con Amazon CloudWatch para que pueda recopilar y analizar las métricas operativas de sus clústeres. Puede supervisar estas métricas mediante la CloudWatch consola, la consola Amazon DocumentDB, AWS Command Line Interface (AWS CLI) o la CloudWatch API.

CloudWatch también le permite configurar alarmas para que se le notifique si el valor de una métrica supera un umbral que especifique. Incluso puedes configurar Amazon CloudWatch Events para que

tome medidas correctivas en caso de que se produzca una infracción. Para obtener más información sobre el uso CloudWatch y las alarmas, consulta la CloudWatch documentación de Amazon.

Temas

- Métricas de Amazon DocumentDB
- Visualización CloudWatch de datos
- Dimensiones de Amazon DocumentDB
- Supervisión de métricas de Opcounter
- Supervisión de conexiones a bases de datos

Métricas de Amazon DocumentDB

Para monitorizar el estado y el rendimiento del clúster e instancias de Amazon DocumentDB, puede consultar las siguientes métricas en la consola de Amazon DocumentDB.

> **Note**
>
> Las métricas de las siguientes tablas se aplican tanto a los clústeres elásticos como a los basados en instancias.

Temas

- Métricas de utilización de recursos
- Métricas de latencia
- NVMe-métricas de instancias respaldadas
- Métricas operativas
- Métricas de rendimiento
- Métricas del sistema
- Métricas de la instancia T3

Métricas de utilización de recursos

Métrica	Description (Descripción)	
`BackupRetentionPeriodStorageUsed`	La cantidad total de almacenamiento de copias de seguridad en bytes utilizada para admitir la función de point-in-time restauración dentro de la ventana de retención de Amazon DocumentDB. Se incluye en el total registrado por la métrica `TotalBackupStorageBilled` . Se calcula de forma independiente para cada clúster de Amazon DocumentDB.	
`ChangeStreamLogSize`	La cantidad de almacenamiento que utiliza el clúster para almacenar el registro de flujos de cambios en megabytes. Este valor es un subconjunto del almacenamiento total del clúster (`VolumeBytesUsed`) y afecta al costo del clúster. Para obtener información acerca de los precios de almacenamiento, consulte la página del producto de Amazon DocumentDB. El tamaño del registro de flujos de cambios es una función que indica la cantidad de cambios que se realizan en el clúster y el periodo en el	

Métrica	Description (Descripción)
	que se conservará dicho registro de flujos de cambios. Para obtener más informaci ón acerca de las secuencias de cambio, consulte Uso de flujos de cambios con Amazon DocumentDB.
`CPUUtilization`	Porcentaje de CPU usado por una instancia.
`DatabaseConnections`	El número de conexiones abiertas (activas e inactivas) en una instancia tomada en una frecuencia de 1 minuto.
`DatabaseConnection sMax`	El número máximo de conexiones abiertas (activas e inactivas) en una instancia en un período de 1 minuto.
`DatabaseConnection sLimit`	El número máximo de conexiones de bases de datos simultáneas (activas e inactivas) permitidas en una instancia en un momento dado.
`DatabaseCursors`	El número de cursores abiertos en una instancia tomados en una frecuencia de 1 minuto.

Métrica	Description (Descripción)
DatabaseCursorsMax	El número máximo de cursores abiertos en una instancia en un período de 1 minuto.
DatabaseCursorsLimit	El número máximo de cursores permitidos en una instancia en un momento dado.
DatabaseCursorsTimedOut	El número de cursores cuyo tiempo de espera se agotó en un período de 1 minuto.
FreeableMemory	Cantidad de memoria de acceso aleatorio disponible en bytes.
FreeLocalStorage	Esta métrica indica la cantidad de almacenamiento disponible en cada instancia para las tablas y los registros temporales. Este valor depende de la clase de instancia. Puede aumentar la cantidad de espacio de almacenamiento libre para una instancia eligiendo una clase de instancia más grande para ella.
LowMemThrottleQueueDepth	La profundidad de la cola para las solicitudes que están limitadas debido a la poca memoria disponible tomada en una frecuencia de 1 minuto.

Métrica	Description (Descripción)
`LowMemThrottleMaxQueueDepth`	La profundidad máxima de la cola para las solicitudes que están limitadas debido a la poca memoria disponible en un período de 1 minuto.
`LowMemNumOperationsThrottled`	El número de solicitudes que están limitadas debido a la poca memoria disponible en un período de 1 minuto.
`SnapshotStorageUsed`	La cantidad total de almacenamiento de copias de seguridad en bytes consumida por todas las instantáneas de un clúster de Amazon DocumentDB determina do fuera de su período de retención de la copia de seguridad. Se incluye en el total registrado por la métrica `TotalBackupStorageBilled` . Se calcula de forma independiente para cada clúster de Amazon DocumentDB.
`SwapUsage`	La cantidad de espacio de intercambio utilizado en la instancia.

Métrica	Description (Descripción)
`TotalBackupStorageBilled`	La cantidad total de almacenamiento de copias de seguridad en bytes facturada para un clúster de Amazon DocumentDB determinado. Incluye el almacenamiento de copias de seguridad medido por las métricas `BackupRetentionPeriodStorageUsed` y `SnapshotStorageUsed`. Se calcula de forma independiente para cada clúster de Amazon DocumentDB.
`TransactionsOpen`	El número de transacciones abiertas en una instancia en una frecuencia de 1 minuto.
`TransactionsOpenMax`	El número máximo de transacciones abiertas en una instancia en un período de 1 minuto.
`TransactionsOpenLimit`	El número máximo de transacciones simultáneas permitidas en una instancia en un momento dado.

Métrica	Description (Descripción)
VolumeBytesUsed	Cantidad de almacenamiento utilizada por el clúster en bytes. Este valor afecta al costo del clúster. Para obtener información acerca de los precios, consulte la página del producto de Amazon DocumentDB.

Métricas de latencia

Métrica	Description (Descripción)
DBClusterReplicaLagMaximum	Retardo máximo en milisegundos entre la instancia principal y cada instancia de base de datos de Amazon DocumentDB del clúster.
DBClusterReplicaLagMinimum	Retardo mínimo en milisegundos entre la instancia principal y cada instancia de réplica del clúster.
DBInstanceReplicaLag	La cantidad de retardo, en milisegundos, cuando la replicación actualiza desde la instancia principal a una instancia de réplica.
ReadLatency	La cantidad media de tiempo que tarda cada I/O operación de disco.

Métrica	Description (Descripción)	
`WriteLatency`	La cantidad media de tiempo, en milisegundos, que se tarda en realizar cada I/O operación de disco.	

NVMe-métricas de instancias respaldadas

Métrica	Description (Descripción)	
`NVMeStorageCacheHitRatio`	El porcentaje de solicitudes que se responden desde la caché por niveles.	
`FreeNVMeStorage`	La cantidad de almacenamiento efímero NVMe disponible.	
`ReadIOPSNVMeStorage`	El número promedio de I/O operaciones de lectura de disco para almacenamiento efímero NVMe .	
`ReadLatencyNVMeStorage`	El tiempo medio que tarda cada I/O operación de lectura de disco en el almacenamiento efímero NVMe .	
`ReadThroughputNVMeStorage`	El número promedio de bytes leídos del disco por segundo para el almacenamiento efímero NVMe .	
`WriteIOPSNVMeStorage`	El número promedio de I/O operaciones de escritura en	

Métrica	Description (Descripción)	
	disco en un almacenamiento efímero NVMe .	
`WriteLatencyNVMeStorage`	El tiempo medio que tarda cada I/O operación de escritura en disco en el almacenamiento efímero NVMe .	
`WriteThroughputNVMeStorage`	El número promedio de bytes escritos en el disco por segundo para el almacenamiento efímero NVMe .	

Métricas operativas

Métrica	Description (Descripción)	
`DocumentsDeleted`	El número de documentos eliminados en un período de 1 minuto.	
`DocumentsInserted`	El número de documentos insertados en un período de 1 minuto.	
`DocumentsReturned`	El número de documentos devueltos en un período de 1 minuto.	
`DocumentsUpdated`	El número de documentos actualizados en un período de 1 minuto.	

Métrica	Description (Descripción)
OpcountersCommand	El número de comandos emitidos en un período de 1 minuto.
OpcountersDelete	El número de operaciones de eliminación emitidas en un período de 1 minuto.
OpcountersGetmore	El número de getmores emitidos en un período de 1 minuto.
OpcountersInsert	El número de operaciones de inserción emitidas en un período de 1 minuto.
OpcountersQuery	El número de consultas emitidas en un período de 1 minuto.
OpcountersUpdate	El número de operaciones de actualización emitidas en un período de 1 minuto.
TransactionsStarted	El número de transacciones iniciadas en una instancia en un período de 1 minuto.
TransactionsCommitted	El número de transacciones realizadas en una instancia en un período de 1 minuto.
TransactionsAborted	El número de transacciones canceladas en una instancia en un período de 1 minuto.

Métrica	Description (Descripción)	
`TTLDeletedDocuments`	El número de documentos eliminados por a TTLMonitor en un período de 1 minuto.	

Métricas de rendimiento

Métrica	Description (Descripción)	
`NetworkReceiveThroughput`	Cantidad de rendimiento de red en bytes por segundo recibida de los clientes por cada instancia del clúster. Este rendimiento no incluye el tráfico de red entre las instancias del clúster y el volumen del clúster.	
`NetworkThroughput`	Cantidad de rendimiento de red en bytes por segundo recibida de los clientes y transmitida a ellos por cada instancia del clúster de Amazon DocumentDB. Este rendimiento no incluye el tráfico de red entre las instancias del clúster y el volumen del clúster.	
`NetworkTransmitThroughput`	Cantidad de rendimiento de red en bytes por segundo enviada a los clientes por cada instancia del clúster de base de datos. Este rendimiento no incluye el tráfico de red	

Métrica	Description (Descripción)	
	entre las instancias del clúster y el volumen del clúster.	
`ReadIOPS`	El número medio de I/O operaciones de lectura del disco por segundo. Amazon DocumentDB indica las IOPS de lectura y escritura por separado, en intervalos de 1 minuto.	
`ReadThroughput`	El número medio de bytes leídos del disco por segundo.	
`StorageNetworkReceiveThroughput`	Cantidad de rendimiento de red en bytes por segundo recibida del volumen de almacenamiento del clúster de Amazon DocumentDB por cada instancia del clúster.	
`StorageNetworkTransmitThroughput`	Cantidad de rendimiento de red en bytes por segundo enviada al volumen de almacenamiento del clúster de Amazon DocumentDB por cada instancia del clúster.	
`StorageNetworkThroughput`	Cantidad de rendimiento de red en bytes por segundo recibida y enviada al volumen de almacenamiento del clúster de Amazon DocumentDB por cada instancia del clúster de Amazon DocumentDB.	

Métrica	Description (Descripción)	
`VolumeReadIOPs`	El número promedio de I/O operaciones de lectura facturadas desde un volumen de clúster, registrado en intervalos de 5 minutos. Las operaciones de lectura facturadas se calculan en el nivel del volumen de clúster, se agrupan para todas las instancias del clúster y se notifican a intervalos de 5 minutos. El valor se calcula tomando el valor de la métrica de operaciones de lectura a lo largo de un periodo de 5 minutos. Puede determina r la cantidad de operacion es de lectura facturadas por segundo tomando el valor de la métrica de operaciones de lectura facturadas y dividiénd ola por 300 segundos. Por ejemplo, si las `VolumeReadIOPs` devuelven 13,686, las operaciones de lectura facturadas por segundo serán 45 (13 686/300 = 45.62). Las operaciones de lectura facturadas se acumulan para las consultas que solicitan páginas de la base de datos que no están presentes en	

Métrica	Description (Descripción)	
	la caché del búfer y que por tanto se deben cargar desde el almacenamiento. Es posible que aparezcan picos en las operaciones de lectura facturadas, ya que los resultados de la consulta se leen desde el almacenamiento y se cargan en la caché del búfer.	

Métrica	Description (Descripción)	
`VolumeWriteIOPs`	El número promedio de I/O operaciones de escritura facturadas desde un volumen de clúster, registrado en intervalos de 5 minutos. Las operaciones de escritura facturadas se calculan en el nivel del volumen de clúster, se agrupan para todas las instancias del clúster y se notifican a intervalos de 5 minutos. El valor se calcula tomando el valor de la métrica de operaciones de escritura a lo largo de un periodo de 5 minutos. Puede determina r la cantidad de operaciones de escritura facturadas por segundo tomando el valor de la métrica de operacion es de escritura facturadas y dividiendo por 300 segundos. Por ejemplo, si las `VolumeWriteIOPs` devuelven 13,686, las operaciones de escritura facturadas por segundo serán 45 (13 686/300 = 45.62). Tenga en cuenta que `VolumeReadIOPs` las `VolumeWriteIOPs` métricas se calculan mediante la capa de almacenamiento	

Métrica	Description (Descripción)	
	de DocumentDB e incluyen las IOs realizadas por las instancias principal y de réplica. Los datos se agregan cada 20 a 30 minutos y después, se generan informes en intervalos de 5 minutos, por lo que se emite el mismo punto de datos para la métrica en el período de tiempo. Si busca una métrica que se correlaci one con tus operaciones de inserción en un intervalo de 1 minuto, puede usar la métrica WriteIOps a nivel de instancia . La métrica está disponible en la pestaña de supervisión de la instancia principal de Amazon DocumentDB.	
`WriteIOPS`	El número promedio de I/O operaciones de escritura en disco por segundo. Cuando se utilizan a nivel de clúster, `WriteIOPs` se evalúan en todas las instancias del clúster. Las IOPS de lectura y escritura se registran por separado, en intervalos de 1 minuto.	
`WriteThroughput`	Número medio de bytes que se escriben en el disco por segundo.	

Métricas del sistema

Métrica	Description (Descripción)	
`AvailableMVCCIds`	Un contador que muestra el número de operaciones de escritura restantes disponibl es antes de llegar a cero. Cuando este contador llegue a cero, el clúster pasará al modo de solo lectura hasta que IDs se recupere y se recicle. El contador disminuye con cada operación de escritura y aumenta a medida que la recolección de basura recicla el MVCC antiguo. IDs	
`BufferCacheHitRatio`	Porcentaje de solicitudes que se responden desde la caché de búfer.	
`DiskQueueDepth`	El número de I/O operacion es que están esperando a escribirse o leerse desde el disco.	
`EngineUptime`	Cantidad de tiempo en segundos que la instancia lleva en ejecución.	
`IndexBufferCacheHi tRatio`	Porcentaje de solicitudes de índice que se responden desde la caché de búfer. Es posible que vea un pico superior al 100 % en la métrica justo después de eliminar un índice, una	

Métrica	Description (Descripción)	
	colección o una base de datos. Esto se resolverá automáticamente después de 60 segundos. Esta limitación se corregirá en una actualización futura del parche.	
`LongestActiveGCRuntime`	Duración en segundos del proceso activo de recopilación de elementos no utilizados más prolongado. Se actualiza cada minuto y realiza un seguimiento únicamente de las operaciones activas, excluyendo los procesos que se completan en el intervalo de un minuto.	

Métricas de la instancia T3

Métrica	Description (Descripción)	
`CPUCreditUsage`	El número total de créditos de CPU que se han gastado durante el periodo de medición.	
`CPUCreditBalance`	El número de créditos de la CPU que ha acumulado una instancia. Este saldo se agota cuando la CPU realiza ráfagas y los créditos de CPU se gastan más rápido de lo que se obtienen.	

Métrica	Description (Descripción)	
`CPUSurplusCreditBalance`	El número de créditos de CPU sobrantes que se utilizan para mantener el rendimiento de la CPU cuando el valor de CPUCredit equilibrio es cero.	
`CPUSurplusCreditsCharged`	El número de créditos de CPU sobrantes que superen la cantidad máxima de créditos de CPU que se pueden obtener en un periodo de 24 horas y que, por lo tanto, generan gastos adicionales. Para obtener más información, consulte Monitoreo de sus créditos CPU.	

Visualización CloudWatch de datos

Puede ver CloudWatch los datos de Amazon mediante la CloudWatch consola, la consola Amazon DocumentDB, AWS Command Line Interface (AWS CLI) o la CloudWatch API.

Using the Consola de administración de AWS

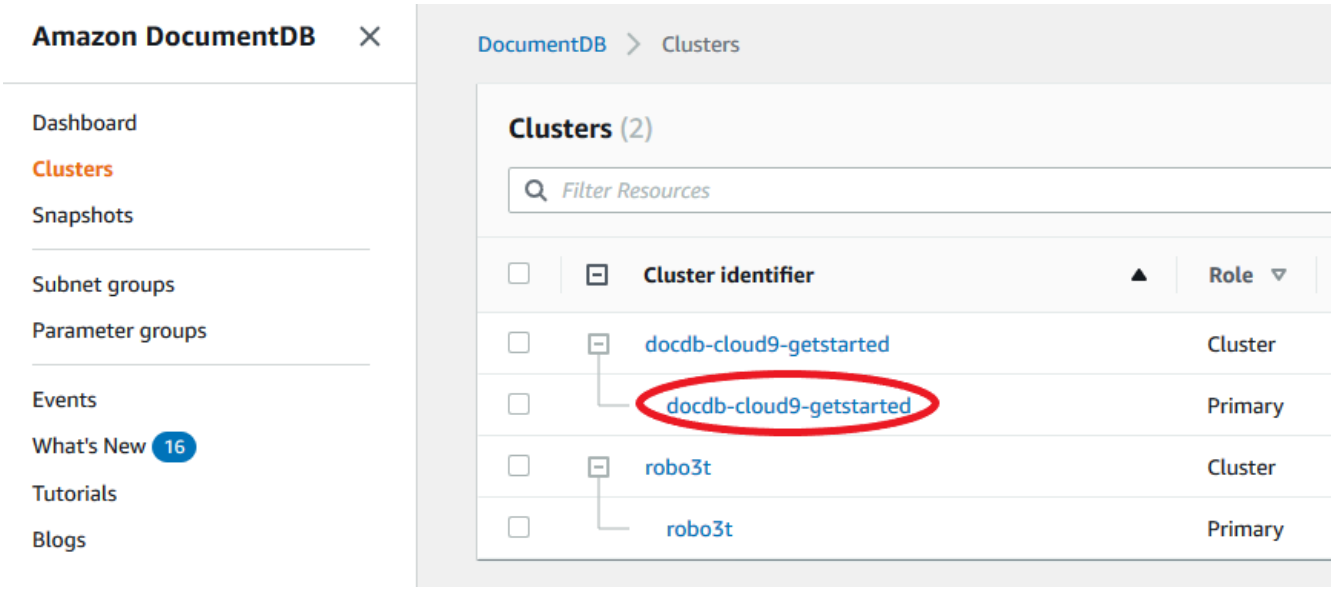
Para ver CloudWatch las métricas mediante la consola de administración de Amazon DocumentDB, complete los siguientes pasos.

1. Inicie sesión en y abra la Consola de administración de AWS consola de Amazon DocumentDB en https://console.aws.amazon.com /docdb.
2. En el panel de navegación, seleccione Clusters (Clústeres).

> **Tip**
>
> Si no ve el panel de navegación del lado izquierdo de la pantalla, seleccione el icono de menú

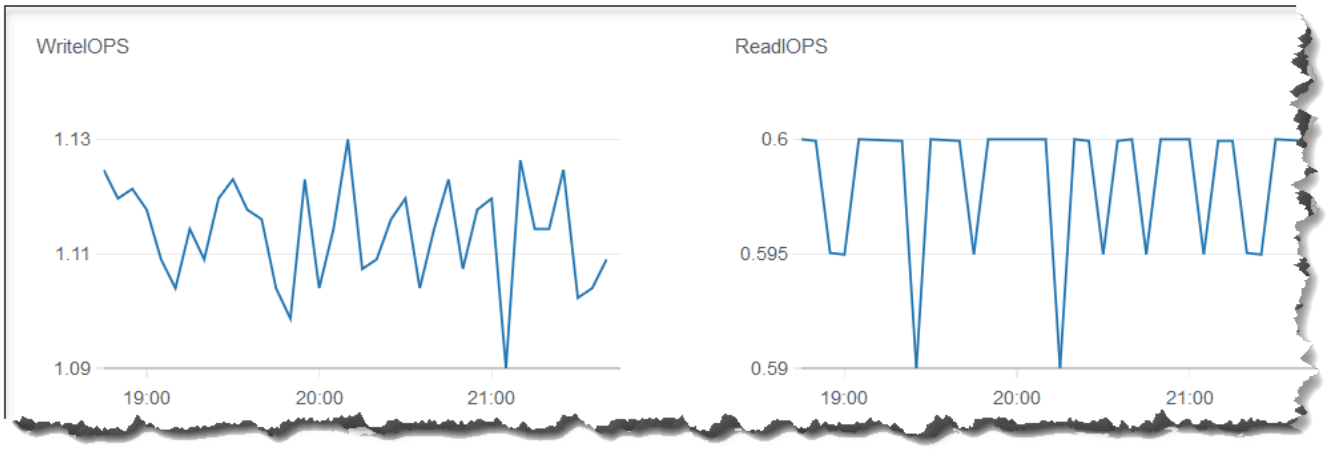
(≡)
en la esquina superior izquierda de la página.

3. En el cuadro de navegación de clústeres, verá la columna Identificador del clúster. Las instancias se muestran en clústeres, de forma similar a la siguiente captura de pantalla.



4. En la lista de instancias, seleccione el nombre de la instancia de la que desea ver las métricas.
5. En la página de resumen de instancias resultante, seleccione la pestaña Monitorización para ver las representaciones gráficas de las métricas de su instancia de Amazon DocumentDB. Como se debe generar un gráfico para cada métrica, los CloudWatchgráficos pueden tardar unos minutos en rellenarse.

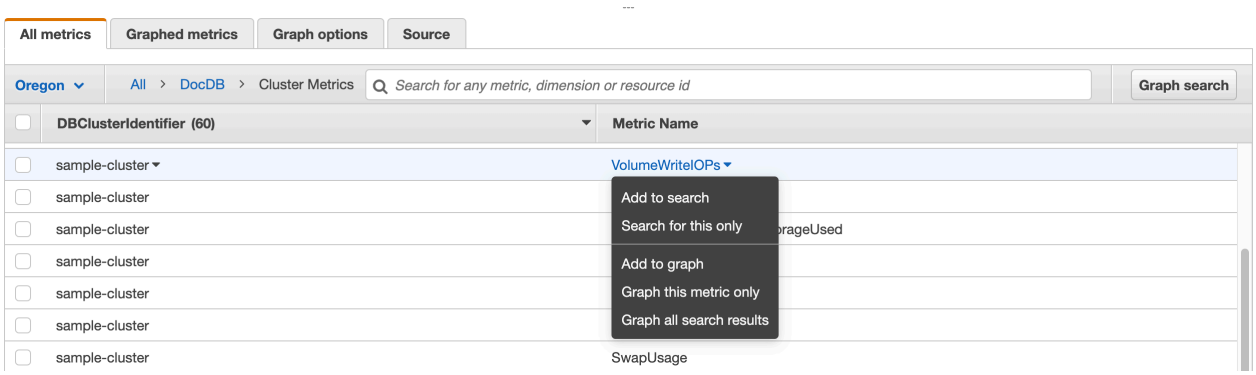
   La siguiente imagen muestra las representaciones gráficas de dos CloudWatch métricas en la consola Amazon DocumentDB y`WriteIOPS`. `ReadIOPS`



Using the CloudWatch Management Console

Para ver CloudWatch las métricas mediante la consola de CloudWatch administración, complete los siguientes pasos.

1. Inicie sesión en y abra la Consola de administración de AWS consola de Amazon DocumentDB en. https://console.aws.amazon.com/cloudwatch
2. En el panel de navegación, seleccione Métricas. A continuación, en la lista de nombres de servicios, elija DocDB.
3. Elija una dimensión de métrica (por ejemplo, Métricas del clúster).
4. La pestaña Todas las métricas muestra todas las métricas para dicha dimensión en DocDB.
   a. Para ordenar la tabla, utilice el encabezado de columna.
   b. Para representar gráficamente una métrica, active la casilla de verificación situada junto a ella. Para seleccionar todas las métricas, seleccione la casilla de verificación en la fila de encabezado de la tabla.
   c. Para filtrar por métrica, coloque el cursor sobre el nombre de la métrica y seleccione la flecha desplegable situada junto al nombre de la métrica. A continuación, selecciona Añadir a la búsqueda, como se muestra en la siguiente imagen.



Using the AWS CLI

Para ver CloudWatch los datos de Amazon DocumentDB, utilice la CloudWatch `get-metric-statistics` operación con los siguientes parámetros.

Parameters

- **`--namespace`**: obligatorio. El espacio de nombres del servicio para el que desea obtener métricas de CloudWatch . Para Amazon DocumentDB, debe ser `AWS/DocDB`.

- **`--metric-name`**: obligatorio. El nombre de la métrica para la que desea obtener datos.
- **`--start-time`**: obligatorio. La marca temporal que determina el primer punto de datos que se va a devolver.

  El valor especificado es inclusivo; los resultados incluyen puntos de datos con la marca temporal especificada. La marca temporal debe estar en el formato UTC ISO 8601 (por ejemplo, 2016-10-03T23:00:00 Z).
- **`--end-time`**: obligatorio. La marca temporal que determina el último punto de datos que se va a devolver.

  El valor especificado es inclusivo; los resultados incluyen puntos de datos con la marca temporal especificada. La marca temporal debe estar en el formato UTC ISO 8601 (por ejemplo, 2016-10-03T23:00:00 Z).
- **`--period`**: obligatorio. El grado de detalle, en segundos, de los puntos de datos devueltos. Para las métricas con una resolución normal, un periodo puede ser tan breve como un minuto (60 segundos) y debe ser un múltiplo de 60. Para las métricas de alta resolución que se recopilan a intervalos de menos de un minuto, el periodo puede ser 1, 5, 10, 30, 60 o cualquier múltiplo de 60.
- **`--dimensions`**— Opcional. Si la métrica contiene varias dimensiones, debe incluir un valor para cada dimensión. CloudWatch trata cada combinación única de dimensiones como una métrica independiente. No se pueden recuperar estadísticas utilizando combinaciones de dimensiones que no se han publicado. Debe especificar las mismas dimensiones que se utilizaron al crear las métricas.
- **`--statistics`**: opcional. La estadística de la métrica, distinta del percentil. Para la estadística de percentil, utilice `ExtendedStatistics`. Cuando llama a `GetMetricStatistics`, debe especificar `Statistics` o `ExtendedStatistics`, pero no ambos.

  Valores permitidos:

  - `SampleCount`
  - `Average`
  - `Sum`
  - `Minimum`
  - `Maximum`

- **`--extended-statistics`**: opcional. La estadística `percentile`. Especifique valores comprendidos entre p0.0 y p100. Cuando llama a `GetMetricStatistics`, debe especificar `Statistics` o `ExtendedStatistics`, pero no ambos.
- **`--unit`**: opcional. La unidad de una métrica determinada. Las métricas se pueden registrar en varias unidades. Si no se especifica una unida, se devuelven todas las unidades. Si especifica solo una unidad que la métrica no registra, los resultados de la llamada son nulos.

  Valores posibles:

  - `Seconds`
  - `Microseconds`
  - `Milliseconds`
  - `Bytes`
  - `Kilobytes`
  - `Megabytes`
  - `Gigabytes`
  - `Terabytes`
  - `Bits`
  - `Kilobytes`
  - `Megabits`
  - `Gigabits`
  - `Terabits`
  - `Percent`
  - `Count`
  - `Bytes/Second`
  - `Kilobytes/Second`
  - `Megabytes/Second`
  - `Gigabytes/Second`
  - `Terabytes/Second`
  - `Bits/Second`
  - `Kilobits/Second`
  - `Megabits/Second`

- `Gigabits/Second`
- `Terabits/Second`
- `Count/Second`
- `None`

Example

En el siguiente ejemplo se busca el valor máximo de `CPUUtilization` para un periodo de 2 horas tomando una muestra cada 60 segundos.

Para Linux, macOS o Unix:

```
aws cloudwatch get-metric-statistics \
       --namespace AWS/DocDB \
       --dimensions \
           Name=DBInstanceIdentifier,Value=docdb-2019-01-09-23-55-38 \
       --metric-name CPUUtilization \
       --start-time 2019-02-11T05:00:00Z \
       --end-time 2019-02-11T07:00:00Z \
       --period 60 \
       --statistics Maximum
```

Para Windows:

```
aws cloudwatch get-metric-statistics ^
       --namespace AWS/DocDB ^
       --dimensions ^
           Name=DBInstanceIdentifier,Value=docdb-2019-01-09-23-55-38 ^
       --metric-name CPUUtilization ^
       --start-time 2019-02-11T05:00:00Z ^
       --end-time 2019-02-11T07:00:00Z ^
       --period 60 ^
       --statistics Maximum
```

La salida de esta operación será similar a lo que se indica a continuación.

```
{
       "Label": "CPUUtilization",
       "Datapoints": [
```

```
            {
                "Unit": "Percent",
                "Maximum": 4.49152542374361,
                "Timestamp": "2019-02-11T05:51:00Z"
            },
            {
                "Unit": "Percent",
                "Maximum": 4.25000000000485,
                "Timestamp": "2019-02-11T06:44:00Z"
            },

            ********* some output omitted for brevity *********

            {
                "Unit": "Percent",
                "Maximum": 4.33333333331878,
                "Timestamp": "2019-02-11T06:07:00Z"
            }
        ]
    }
```

Dimensiones de Amazon DocumentDB

Las métricas de Amazon DocumentDB se identifican por los valores de la cuenta o de la operación. Puede utilizar la CloudWatch consola para recuperar los datos de Amazon DocumentDB filtrados por cualquiera de las dimensiones de la tabla siguiente.

Dimensión	Description (Descripción)
`DBClusterIdentifier`	Filtra los datos solicitados que son específicos del clúster de Amazon DocumentDB.
`DBClusterIdentifier, Role`	Filtra los datos solicitados para un clúster de Amazon DocumentDB específico, agrupando las métricas por rol de instancia (WRITER/READER). Por ejemplo, puede agregar métricas para todas las instancias READER que pertenezcan a un clúster.

Dimensión	Description (Descripción)
`DBInstanceIdentifier`	Filtra los datos solicitados para una instancia de base de datos específica.

Supervisión de métricas de Opcounter

Las métricas de Opcounter tienen un valor distinto de cero (normalmente ~ 50) para los clústeres inactivos. Esto se debe a que Amazon DocumentDB realiza comprobaciones de estado periódicas, operaciones internas y tareas de recopilación de métricas.

Supervisión de conexiones a bases de datos

Al ver el número de conexiones mediante comandos del motor de base de datos, por ejemplo`db.runCommand( { serverStatus: 1 })`, es posible que vea hasta 10 conexiones más de las que ve. `DatabaseConnections` CloudWatch Esto ocurre porque Amazon DocumentDB realiza comprobaciones de estado periódicas y tareas de recopilación de métricas que no se tienen en cuenta en `DatabaseConnections`. `DatabaseConnections` representa únicamente las conexiones iniciadas por el cliente.

Registro de llamadas a la API de Amazon DocumentDB con AWS CloudTrail

Amazon DocumentDB (con compatibilidad con MongoDB) se integra con AWS CloudTrail, un servicio que proporciona un registro de las medidas adoptadas por un usuario, un rol o un servicio de AWS en Amazon DocumentDB (compatible con MongoDB). CloudTrail obtiene todas las llamadas a la AWS CLI API para Amazon DocumentDB como eventos, incluidas las llamadas procedentes de la consola de Amazon DocumentDB y de las llamadas de código de la SDK de Amazon DocumentDB. Si crea un registro de seguimiento, puede habilitar la entrega continua de eventos de CloudTrail a un bucket de Amazon S3, incluidos los eventos de Amazon DocumentDB. Si no configura un registro de seguimiento, puede ver los eventos más recientes en la consola de CloudTrail en el Historial de eventos. Mediante la información que CloudTrail recopila, se puede determinar la petición que se envió a Amazon DocumentDB (con compatibilidad con MongoDB), la dirección IP desde la que se realizó la petición, quién la realizó, cuándo se realizó y otros detalles adicionales.

> **Important**
>
> Para determinadas funciones de administración, Amazon DocumentDB utiliza tecnología operativa que se comparte con Amazon Relational Database Service (Amazon RDS). Las llamadas a la consola de Amazon DocumentDB, la AWS CLI y la API se registran como llamadas realizadas a la API de Amazon RDS.

Para obtener más información sobre AWS CloudTrail, consulte la Guía del usuario de AWS CloudTrail.

Información de Amazon DocumentDB en CloudTrail

CloudTrail se habilita en su Cuenta de AWS cuando se crea la cuenta. Cuando se produce una actividad en Amazon DocumentDB (con compatibilidad con MongoDB), dicha actividad se registra en un evento de CloudTrail junto con los eventos de los demás servicios de AWS en Historial de eventos. Puede ver, buscar y descargar eventos recientes en su Cuenta de AWS. Para obtener más información, consulte Ver eventos con el historial de eventos de CloudTrail.

Para mantener un registro continuo de los eventos en su Cuenta de AWS, incluidos los eventos de Amazon DocumentDB (con compatibilidad con MongoDB), cree un registro de seguimiento. Un registro de seguimiento permite a CloudTrail enviar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las Regiones de AWS. El registro de seguimiento registra los eventos de todas las regiones de la partición de AWS y envía los archivos de registro al bucket de Amazon S3 especificado. También es posible configurar otros servicios de AWS para analizar en profundidad y actuar en función de los datos de eventos recopilados en los registros de CloudTrail. Para obtener más información, consulte los siguientes temas en la Guía del usuario de AWS CloudTrail:

- Introducción a la creación de registros de seguimiento
- Consulte Servicios e integraciones compatibles con CloudTrail
- Configuración de notificaciones de Amazon SNS para CloudTrail
- Recepción de archivos de registro de CloudTrail de multirregiones
- Recepción de archivos de registro de CloudTrail de varias cuentas

Cada entrada de registro o evento incluye información acerca de quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con las credenciales raíz o del usuario.
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro servicio de AWS.

Para obtener más información, consulte el Elemento userIdentity de CloudTrail.

Creación de perfiles de operaciones en Amazon DocumentDB

Puede utilizar el generador de perfiles en Amazon DocumentDB (con compatibilidad con MongoDB) para registrar el tiempo de ejecución y los detalles de las operaciones realizadas en el clúster. El generador de perfiles es útil para monitorizar las operaciones más lentas del clúster para ayudarle a mejorar el rendimiento de las consultas individuales y el rendimiento general del clúster.

De forma predeterminada, la característica del generador de perfiles está deshabilitada. Cuando está habilitada, el generador de perfiles registra las operaciones que tardan más que un valor de umbral definido por el cliente (por ejemplo, 100 ms) en Registros de Amazon CloudWatch. Los detalles registrados incluyen el comando con perfil, la hora, el resumen del plan y los metadatos del cliente. Después de que las operaciones se registren en CloudWatch Logs, puede utilizar CloudWatch Logs Insights para analizar, monitorizar y archivar los datos de perfiles de Amazon DocumentDB. En la sección se proporcionan consultas comunes Consultas comunes.

Cuando está habilitado, el generador de perfiles utiliza recursos adicionales en el clúster. Le recomendamos que comience con un valor de umbral alto (por ejemplo, 500 ms) y que reduzca gradualmente el valor para identificar las operaciones lentas. Comenzar con un valor umbral de 50 ms puede provocar problemas de rendimiento en el clúster para aplicaciones de alto rendimiento. El generador de perfiles está habilitado en el nivel de clúster y funciona en todas las instancias y bases de datos de un clúster. Amazon DocumentDB registra las operaciones en los Registros de Amazon CloudWatch en la medida en que sea posible.

Aunque Amazon DocumentDB no impone ningún recargo adicional para habilitar el generador de perfiles, se le cobrarán tarifas estándar por el uso de CloudWatch Logs. Para obtener más información sobre los precios de CloudWatch Logs, consulte Precios de Amazon CloudWatch.

Temas

- Operaciones admitidas
- Limitaciones

- Habilitación del generador de perfiles de Amazon DocumentDB
- Deshabilitación del generador de perfiles de Amazon DocumentDB
- Deshabilitación de la exportación de registros del generador de perfiles
- Acceso a los registros del generador de perfiles de Amazon DocumentDB
- Consultas comunes

Operaciones admitidas

El generador de perfiles de Amazon DocumentDB admite las siguientes operaciones:

- `aggregate`
- `count`
- `delete`
- `distinct`
- `find` (OP_QUERY y comando)
- `findAndModify`
- `insert`
- `update`

Limitaciones

El generador de perfiles de consultas lento solo puede emitir registros del generador de perfiles si todo el conjunto de resultados de la consulta puede caber en un lote y si el conjunto de resultados es inferior a 16 MB (tamaño máximo de BSON). Los conjuntos de resultados de más de 16 MB se dividen automáticamente en varios lotes.

La mayoría de los controladores o carcasas pueden establecer un tamaño de lote predeterminado que sea pequeño. Puede especificar el tamaño del lote como parte de su consulta. Con el fin de capturar registros de consultas lentos, recomendamos un tamaño de lote que supere el tamaño del conjunto de resultados esperado. Si no está seguro del tamaño del conjunto de resultados o si varía, también puede establecer el tamaño del lote en un número grande (por ejemplo, 100 000).

Sin embargo, si se utiliza un tamaño de lote mayor, será necesario recuperar más resultados de la base de datos antes de enviar una respuesta al cliente. En el caso de algunas consultas, esto puede provocar demoras más prolongadas antes de obtener los resultados. Si no planea consumir todo

el conjunto de resultados, es posible que dedique más E/S a procesar la consulta y desperdiciar el resultado.

Habilitación del generador de perfiles de Amazon DocumentDB

Habilitar el generador de perfiles en un clúster es un proceso de tres pasos. Asegúrese de que todos los pasos se completan o los registros de creación de perfiles no se enviarán a CloudWatch Logs. El generador de perfiles se establece en el nivel de clúster y se realiza en todas las bases de datos e instancias del clúster.

Habilitación del generador de perfiles en un clúster

1. Dado que no puede modificar un grupo de parámetros de clúster predeterminado, asegúrese de que dispone de un grupo de parámetros de clúster personalizado disponible. Para obtener más información, consulte Creación de grupos de parámetros de clúster de Amazon DocumentDB.
2. Con un grupo de parámetros de clúster personalizado disponible, modifique los siguientes parámetros: `profiler`, `profiler_threshold_ms` y `profiler_sampling_rate`. Para obtener más información, consulte Modificación de grupos de parámetros de clúster de Amazon DocumentDB.
3. Cree o modifique el clúster para utilizar el grupo de parámetros de clúster personalizado y para habilitar la exportación de registros de `profiler` a CloudWatch Logs.

En las secciones siguientes se muestra cómo implementar estos pasos mediante la Consola de administración de AWS y la AWS Command Line Interface (AWS CLI).

Using the Consola de administración de AWS

1. Antes de comenzar, cree un clúster de Amazon DocumentDB y un grupo de parámetros de clúster personalizado si aún no tiene uno. Para obtener más información, consulte Creación de grupos de parámetros de clúster de Amazon DocumentDB y Creación de un clúster de Amazon DocumentDB.
2. Utilice un grupo de parámetros de clúster personalizado disponible para modificar los siguientes parámetros. Para obtener más información, consulte Modificación de grupos de parámetros de clúster de Amazon DocumentDB.

   - `profiler`: habilita o deshabilita la creación de perfiles de consultas. Los valores permitidos son `enabled` y `disabled`. El valor predeterminado es `disabled`. Para habilitar la creación de perfiles, establezca el valor en `enabled`.

- `profiler_threshold_ms`: cuando `profiler` se establece en `enabled`, todos los comandos que tardan más que `profiler_threshold_ms` se registran en CloudWatch. Los valores permitidos son `[50-INT_MAX]`. El valor predeterminado es `100`.
- `profiler_sampling_rate`: la fracción de las operaciones lentas que deben registrarse o crear un perfil. Los valores permitidos son `[0.0-1.0]`. El valor predeterminado es `1.0`.

3. Modifique el clúster para utilizar el grupo de parámetros de clúster personalizado y establezca las exportaciones de registro del generador de perfiles para publicar en Amazon CloudWatch.

   a. En el panel de navegación, elija Clusters (Clústeres) para agregar el grupo de parámetros personalizado a un clúster.

   b. Elija el botón situado a la izquierda del nombre del clúster al que desea asociar el grupo de parámetros. Seleccione Actions (Acciones) y, a continuación, Modify (Modificar) para modificar el clúster.

   c. En Cluster options (Opciones de clúster), elija el grupo de parámetros personalizados del paso anterior para agregárselo al clúster.

   d. En Exportaciones de registros, seleccione Registros del generador de perfiles para publicar en Amazon CloudWatch.

   e. Elija Continue (Continuar) para ver un resumen de las modificaciones.

   f. Después de verificar los cambios, puede aplicarlos inmediatamente o durante el siguiente período de mantenimiento en Scheduling of modifications (Programación de modificaciones).

   g. Elija Modify cluster (Modificar clúster) para actualizar el clúster con el nuevo grupo de parámetros.

Using the AWS CLI

El siguiente procedimiento habilita el generador de perfiles en todas las operaciones admitidas para el clúster `sample-cluster`.

1. Antes de comenzar, asegúrese de tener un grupo de parámetros de clúster personalizado disponible; para ello, ejecute el siguiente comando y revise el resultado de un grupo de parámetros de clúster cuyo nombre no contenga `default` y cuya familia de grupos de parámetros sea `docdb3.6`. Si no tiene un grupo de parámetros de clúster distinto

del predeterminado, consulte Creación de grupos de parámetros de clúster de Amazon DocumentDB.

```
aws docdb describe-db-cluster-parameter-groups \
    --query 'DBClusterParameterGroups[*].
[DBClusterParameterGroupName,DBParameterGroupFamily]'
```

En el siguiente resultado, solo `sample-parameter-group` cumple ambos criterios.

```
[
       [
           "default.docdb3.6",
           "docdb3.6"
       ],
       [
           "sample-parameter-group",
           "docdb3.6"
       ]
]
```

2. Utilizando el grupo de parámetros de clúster personalizado, modifique los siguientes parámetros:

   - `profiler`: habilita o deshabilita la creación de perfiles de consultas. Los valores permitidos son `enabled` y `disabled`. El valor predeterminado es `disabled`. Para habilitar la creación de perfiles, establezca el valor en `enabled`.
   - `profiler_threshold_ms`: cuando `profiler` se establece en `enabled`, todos los comandos que tardan más que `profiler_threshold_ms` se registran en CloudWatch. Los valores permitidos son `[50-INT_MAX]`. El valor predeterminado es `100`.
   - `profiler_sampling_rate`: la fracción de las operaciones lentas que deben registrarse o crear un perfil. Los valores permitidos son `[0.0-1.0]`. El valor predeterminado es `1.0`.

```
aws docdb modify-db-cluster-parameter-group \
    --db-cluster-parameter-group-name sample-parameter-group \
    --parameters
 ParameterName=profiler,ParameterValue=enabled,ApplyMethod=immediate \

 ParameterName=profiler_threshold_ms,ParameterValue=100,ApplyMethod=immediate \
```

```
 ParameterName=profiler_sampling_rate,ParameterValue=0.5,ApplyMethod=immediate
```

3. Modifique el clúster de Amazon DocumentDB para que utilice el grupo de parámetros de clúster personalizado `sample-parameter-group` del paso anterior y establezca el parámetro `--enable-cloudwatch-logs-exports` a `profiler`.

   El código siguiente modifica el clúster `sample-cluster` para utilizar el `sample-parameter-group` del paso anterior y agrega `profiler` a las exportaciones habilitadas de CloudWatch Logs.

   ```
   aws docdb modify-db-cluster \
          --db-cluster-identifier sample-cluster \
          --db-cluster-parameter-group-name sample-parameter-group \
          --cloudwatch-logs-export-configuration '{"EnableLogTypes":["profiler"]}'
   ```

   La salida de esta operación será similar a lo que se indica a continuación.

   ```
   {
       "DBCluster": {
           "AvailabilityZones": [
               "us-east-1c",
               "us-east-1b",
               "us-east-1a"
           ],
           "BackupRetentionPeriod": 1,
           "DBClusterIdentifier": "sample-cluster",
           "DBClusterParameterGroup": "sample-parameter-group",
           "DBSubnetGroup": "default",
           "Status": "available",
           "EarliestRestorableTime": "2020-04-07T02:05:12.479Z",
           "Endpoint": "sample-cluster.node.us-east-1.docdb.amazonaws.com",
           "ReaderEndpoint": "sample-cluster.node.us-east-1.docdb.amazonaws.com",
           "MultiAZ": false,
           "Engine": "docdb",
           "EngineVersion": "3.6.0",
           "LatestRestorableTime": "2020-04-08T22:08:59.317Z",
           "Port": 27017,
           "MasterUsername": "test",
           "PreferredBackupWindow": "02:00-02:30",
           "PreferredMaintenanceWindow": "tue:09:50-tue:10:20",
   ```

```
        "DBClusterMembers": [
            {
                "DBInstanceIdentifier": "sample-instance-1",
                "IsClusterWriter": true,
                "DBClusterParameterGroupStatus": "in-sync",
                "PromotionTier": 1
            },
            {
                "DBInstanceIdentifier": "sample-instance-2",
                "IsClusterWriter": true,
                "DBClusterParameterGroupStatus": "in-sync",
                "PromotionTier": 1
            }
        ],
        "VpcSecurityGroups": [
            {
                "VpcSecurityGroupId": "sg-abcd0123",
                "Status": "active"
            }
        ],
        "HostedZoneId": "ABCDEFGHIJKLM",
        "StorageEncrypted": true,
        "KmsKeyId": "arn:aws:kms:us-east-1:<accountID>:key/sample-key",
        "DbClusterResourceId": "cluster-ABCDEFGHIJKLMNOPQRSTUVWXYZ",
        "DBClusterArn": "arn:aws:rds:us-east-1:<accountID>:cluster:sample-
cluster",
        "AssociatedRoles": [],
        "ClusterCreateTime": "2020-01-10T22:13:38.261Z",
        "EnabledCloudwatchLogsExports": [
            "profiler"
        ],
        "DeletionProtection": true
    }
}
```

Deshabilitación del generador de perfiles de Amazon DocumentDB

Para deshabilitar el generador de perfiles, deshabilite tanto el parámetro `profiler` como la exportación de registros de `profiler` a CloudWatch Logs.

Deshabilitación del generador de perfiles

Puede deshabilitar el parámetro `profiler` mediante la Consola de administración de AWS o la AWS CLI, como se indica a continuación.

Using the Consola de administración de AWS

El siguiente procedimiento utiliza la Consola de administración de AWS para deshabilitar Amazon DocumentDB `profiler`.

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon DocumentDB en https://console.aws.amazon.com/docdb.
2. En el panel de navegación, seleccione Grupos de parámetros. A continuación, elija el nombre del grupo de parámetros de clúster en el que desea deshabilitar el generador de perfiles.
3. En la página Cluster parameters (Parámetros de clúster) resultante, seleccione el botón situado a la izquierda del parámetro `profiler` y elija Edit (Editar).
4. En el cuadro de diálogo Modify profiler (Modificar generador de perfiles), elija `disabled` en la lista.
5. Elija Modify cluster parameter (Modificar el parámetro de clúster).

Using the AWS CLI

Para deshabilitar `profiler` en un clúster mediante la AWS CLI, modifique el clúster tal y como se muestra a continuación.

```
aws docdb modify-db-cluster-parameter-group \
    --db-cluster-parameter-group-name sample-parameter-group \
    --parameters
 ParameterName=profiler,ParameterValue=disabled,ApplyMethod=immediate
```

Deshabilitación de la exportación de registros del generador de perfiles

Puede deshabilitar la exportación de registros de `profiler` a CloudWatch Logs mediante la Consola de administración de AWS o la AWS CLI, como se indica a continuación.

Using the Consola de administración de AWS

El siguiente procedimiento utiliza la Consola de administración de AWS para deshabilitar la exportación de registros de Amazon DocumentDB a CloudWatch.

1. Abra la consola de Amazon DocumentDB en https://console.aws.amazon.com/docdb.
2. En el panel de navegación, seleccione Clusters (Clústeres). Elija el botón situado a la izquierda del nombre del clúster para el que desea deshabilitar la exportación de registros.
3. En el menú Actions (Acciones), elija Modify (Modificar).
4. Desplácese hacia abajo hasta la sección Log exports (Exportaciones de registros) y desactive Profiler logs (Registros del generador de perfiles).
5. Elija Continuar.
6. Revise los cambios y, a continuación, elija cuándo desea que se aplique este cambio en su clúster:
   - Apply during the next scheduled maintenance window (Aplicar durante el siguiente periodo de mantenimiento programado
   - Apply immediately (Aplicar inmediatamente
7. Elija Modificar clúster.

Using the AWS CLI

El siguiente código modifica el clúster `sample-cluster` y deshabilita los registros del generador de perfiles de CloudWatch.

Example

Para Linux, macOS o Unix:

```
aws docdb modify-db-cluster \
   --db-cluster-identifier sample-cluster \
   --cloudwatch-logs-export-configuration '{"DisableLogTypes":["profiler"]}'
```

Para Windows:

```
aws docdb modify-db-cluster ^
   --db-cluster-identifier sample-cluster ^
   --cloudwatch-logs-export-configuration '{"DisableLogTypes":["profiler"]}'
```

La salida de esta operación será similar a lo que se indica a continuación.


```
{
    "DBCluster": {
        "AvailabilityZones": [
            "us-east-1c",
            "us-east-1b",
            "us-east-1a"
        ],
        "BackupRetentionPeriod": 1,
        "DBClusterIdentifier": "sample-cluster",
        "DBClusterParameterGroup": "sample-parameter-group",
        "DBSubnetGroup": "default",
        "Status": "available",
        "EarliestRestorableTime": "2020-04-08T02:05:17.266Z",
        "Endpoint": "sample-cluster.node.us-east-1.docdb.amazonaws.com",
        "ReaderEndpoint": "sample-cluster.node.us-east-1.docdb.amazonaws.com",
        "MultiAZ": false,
        "Engine": "docdb",
        "EngineVersion": "3.6.0",
        "LatestRestorableTime": "2020-04-09T05:14:44.356Z",
        "Port": 27017,
        "MasterUsername": "test",
        "PreferredBackupWindow": "02:00-02:30",
        "PreferredMaintenanceWindow": "tue:09:50-tue:10:20",
        "DBClusterMembers": [
            {
                "DBInstanceIdentifier": "sample-instance-1",
                "IsClusterWriter": true,
                "DBClusterParameterGroupStatus": "in-sync",
                "PromotionTier": 1
            },
            {
                "DBInstanceIdentifier": "sample-instance-2",
                "IsClusterWriter": true,
                "DBClusterParameterGroupStatus": "in-sync",
                "PromotionTier": 1
            }
        ],
        "VpcSecurityGroups": [
            {
                "VpcSecurityGroupId": "sg-abcd0123",
                "Status": "active"
            }
```

```
        ],
        "HostedZoneId": "ABCDEFGHIJKLM",
        "StorageEncrypted": true,
        "KmsKeyId": "arn:aws:kms:us-east-1:<accountID>:key/sample-key",
        "DbClusterResourceId": "cluster-ABCDEFGHIJKLMNOPQRSTUVWXYZ",
        "DBClusterArn": "arn:aws:rds:us-east-1:<accountID>:cluster:sample-cluster",
        "AssociatedRoles": [],
        "ClusterCreateTime": "2020-01-10T22:13:38.261Z",
        "DeletionProtection": true
    }
}
```

Acceso a los registros del generador de perfiles de Amazon DocumentDB

Siga estos pasos para acceder a sus registros de perfil de Amazon CloudWatch.

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. Asegúrese de que se encuentra en la misma región que el clúster de Amazon DocumentDB.
3. En el panel de navegación, elija Logs (Registros).
4. Para encontrar los registros del generador de perfiles de su clúster, en la lista, elija `/aws/docdb/`*`yourClusterName`*`/profiler`.

   Los registros de perfil de cada una de las instancias están disponibles debajo de los nombres de instancia respectivos.

Consultas comunes

A continuación se muestran algunas consultas comunes que puede utilizar para analizar los comandos con perfil. Para obtener más información sobre CloudWatch Logs Insights, consulte Análisis de datos de registro con CloudWatch Logs Insights y las Consultas de muestra.

Obtención de las 10 operaciones más lentas en una colección especificada

```
filter ns="test.foo" | sort millis desc | limit 10
```

Obtención de todas las operaciones de actualización de una colección que tardaron más de 60 ms

```
filter millis > 60 and op = "update"
```

Obtención de las 10 operaciones más lentas del último mes

```
sort millis desc | limit 10
```

Obtener todas las consultas con un resumen de plan COLLSCAN

```
filter planSummary="COLLSCAN"
```

Supervisión con información sobre rendimiento

Información sobre rendimiento amplía las características de monitorización existentes de Amazon DocumentDB para ilustrar el desempeño de su clúster y le ayuda a analizar cualquier problema que le afecte. Con el panel de Información sobre rendimiento, puede visualizar la carga de la base de datos y filtrarla por esperas, instrucciones de consulta, hosts o usuarios.

> **Note**
>
> Información sobre rendimiento solo está disponible para los clústeres basados en instancias de Amazon DocumentDB 3.6, 4.0 y 5.0.

¿Para qué sirve?

- Visualice el rendimiento de la base de datos: visualice la carga para determinar cuándo y dónde se encuentra la carga en la base de datos
- Determine la causa de la carga en la base de datos: determine qué consultas, hosts y aplicaciones contribuyen a la carga de la instancia
- Determine cuándo hay carga en su base de datos: amplíe el panel de Información sobre rendimiento para centrarse en eventos específicos o reduzca el tamaño para observar las tendencias a lo largo de un período de tiempo más amplio

- Alerta sobre la carga de la base de datos: acceda automáticamente a las nuevas métricas de carga de la base de datos desde CloudWatch donde podrá monitorizar las métricas de carga de la base de datos junto con otras métricas de Amazon DocumentDB y establecer alertas en ellas.

¿Cuáles son las limitaciones de Información sobre rendimiento de Amazon DocumentDB?

- Performance Insights en las regiones AWS GovCloud (EE. UU. Este) y AWS GovCloud (EE. UU. Oeste) no están disponibles
- La Información sobre rendimiento para Amazon DocumentDB retiene hasta 7 días de datos de rendimiento
- Las consultas de más de 1024 bytes no se agregan en Información sobre rendimiento

Temas

- Conceptos de Información sobre rendimiento
- Activación y desactivación de Información sobre rendimiento
- Configuración de directivas de acceso para información sobre rendimiento
- Análisis de métricas mediante el panel de Información sobre rendimiento
- Recuperación de métricas con la API de Información sobre rendimiento
- CloudWatch Métricas de Amazon para Performance Insights
- Métricas de contador para Información sobre rendimiento

Conceptos de Información sobre rendimiento

Temas

- Sesiones activas promedio
- Dimensiones
- Max vCPU

Sesiones activas promedio

La carga de base de datos mide el nivel de actividad en la base de datos. La métrica clave en Información sobre rendimiento es `DB Load`, que se recopila cada segundo. La unidad para la métrica `DBLoad` es el promedio de sesiones activas (AAS) de la instancia de Amazon DocumentDB.

Una sesión activa es una conexión que ha enviado trabajo a la instancia de Amazon DocumentDB y está esperando una respuesta. Por ejemplo, si envía una consulta a una instancia de Amazon DocumentDB, la sesión de base de datos estará activa mientras el motor de base de datos procesa la consulta.

Para obtener un promedio de sesiones activas, la Información sobre rendimiento muestrea el número de sesiones que ejecutan una consulta al mismo tiempo. El AAS es el total del número de sesiones dividido entre el total del número de muestras. En la tabla siguiente se muestran 5 ejemplos consecutivos de una consulta en ejecución.

Ejemplo	Número de sesiones que ejecutan una consulta	AAS	Cálculo
1	2	2	2 sesiones / 1 muestra
2	0	1	2 sesiones / 2 muestras
3	4	2	6 sesiones / 3 muestras
4	0	1.5	6 sesiones / 4 muestras
5	4	2	10 sesiones / 5 muestras

En el ejemplo anterior, la carga de base de datos para el intervalo de tiempo de 1 a 5 es 2 AAS. Un aumento en la carga de base de datos significa que, en promedio, se están ejecutando más sesiones en la base de datos.

Dimensiones

La métrica `DB Load` es distinta de las demás métricas de series temporales porque puede desglosarla en subcomponentes llamados dimensiones. Las dimensiones son una especie de

categorías de las diferentes características de la métrica DB Load. Cuando se diagnostican problemas de rendimiento, las dimensiones más útiles son los eventos de espera y top SQL.

estados de espera

Un evento de espera hace que una instrucción de consulta espere a que ocurra un evento específico antes de que pueda continuar ejecutándose. Por ejemplo, una instrucción de consulta podría esperar hasta que se desbloqueara un recurso bloqueado. Al combinar DB Load con eventos de espera, puede obtener una imagen completa del estado de la sesión. Estos son varios estados de espera de Amazon DocumentDB:

Estado de espera de Amazon DocumentDB	Descripción del estado de espera
Pestillo	El estado de espera de pestillo se produce cuando la sesión está esperando para paginar el conjunto de búferes. La entrada y salida frecuentes del conjunto de búferes puede producirse con mayor frecuencia cuando el sistema procesa consultas frecuentes de gran tamaño, escanea colecciones o cuando el grupo de búferes es demasiado pequeño para gestionar todo el conjunto de trabajo.
CPU	El estado de espera de la CPU se produce cuando la sesión está esperando en la CPU.
CollectionLock	El estado de CollectionLock espera se produce cuando la sesión está esperando a que se bloquee la colección. Estos eventos se producen cuando hay operaciones de DDL en la colección.
DocumentLock	El estado de DocumentLock espera se produce cuando la sesión está esperando a que se bloquee un documento. Un número elevado de escrituras simultáneas en el mismo documento contribuirá a que haya más estados de DocumentLock espera en ese documento.

Estado de espera de Amazon DocumentDB	Descripción del estado de espera
SystemLock	El estado de SystemLock espera se produce cuando la sesión está en espera en el sistema. Esto puede ocurrir cuando hay consultas frecuentes de larga duración, transacciones de larga duración o mucha simultaneidad en el sistema.
E/S	El estado de espera de la E/S se produce cuando la sesión está esperando en la E/S.
BufferLock	El estado de BufferLock espera se produce cuando la sesión está esperando a que se bloquee una página compartida del búfer. BufferLockLos estados de espera pueden prolongarse si otros procesos mantienen los cursores abiertos en las páginas solicitadas.
LowMemThrottle	El estado de LowMemThrottle espera se produce cuando la sesión está en espera debido a una gran presión de memoria en la instancia de Amazon DocumentDB. Si este estado persiste durante mucho tiempo, considere la posibilidad de escalar verticalm ente la instancia para proporcionar memoria adicional. Para obtener más información, consulte Recurso de origen.
BackgroundActivity	El estado de BackgroundActivity espera se produce cuando la sesión está en espera de un proceso interno del sistema.

Estado de espera de Amazon DocumentDB	Descripción del estado de espera
Otro	El otro estado de espera es un estado de espera interno. Si este estado persiste durante mucho tiempo, considere la posibilidad de finalizar esta consulta. Para obtener más información, consulte ¿Cómo puedo encontrar y terminar las consultas que tardan mucho en ejecutarse o se bloquean?

Consultas principales

Mientras que los eventos de espera muestran los cuellos de botella, las consultas principales indican qué consultas están contribuyendo más a la carga de la base de datos. Por ejemplo, es posible que, aunque haya muchas consultas ejecutándose actualmente en la base de datos, una de ellas consuma el 99 % de la carga de la base de datos. En este caso, es posible que la carga alta indique un problema con la consulta.

Max vCPU

En el panel, el gráfico de Carga de base de datos recopila, agrega y muestra información de la sesión. Para ver si las sesiones activas superan el máximo de la CPU, observe su relación con la línea Máximo de la CPU virtual. El valor Máximo de la vCPU se determina por el número de núcleos de vCPU (CPU virtual) de la instancia de Amazon DocumentDB.

Si la carga de base de datos suele estar por encima de la línea Máximo de la CPU virtual y el estado de espera principal es CPU, la CPU del sistema está sobrecargada. En este caso, quizá sea conveniente limitar las conexiones con la instancia, ajustar las consultas con una carga de CPU alta o pensar en la posibilidad de usar una clase de instancia de mayor tamaño. Si hay instancias altas y uniformes en cualquier estado de espera, eso indica que es posible que haya problemas de contención de recursos o cuellos de botella que hay que resolver. Esto puede ser así aunque la carga de base de datos no cruce la línea de Máximo de la CPU virtual.

Activación y desactivación de Información sobre rendimiento

Para poder usar Información sobre rendimiento, debe activarlo en su instancia de base de datos. Si lo necesita, podrá desactivarlo más adelante. La activación y desactivación de Información sobre rendimiento no provoca tiempos de inactividad, un reinicio o una conmutación por error.

El agente Información sobre rendimiento consume CPU y memoria limitadas en el host de base de datos. Cuando la carga de la base de datos es alta, el agente limita el impacto en el rendimiento mediante la recopilación de datos con menos frecuencia.

Activación de Información sobre rendimiento al crear un clúster

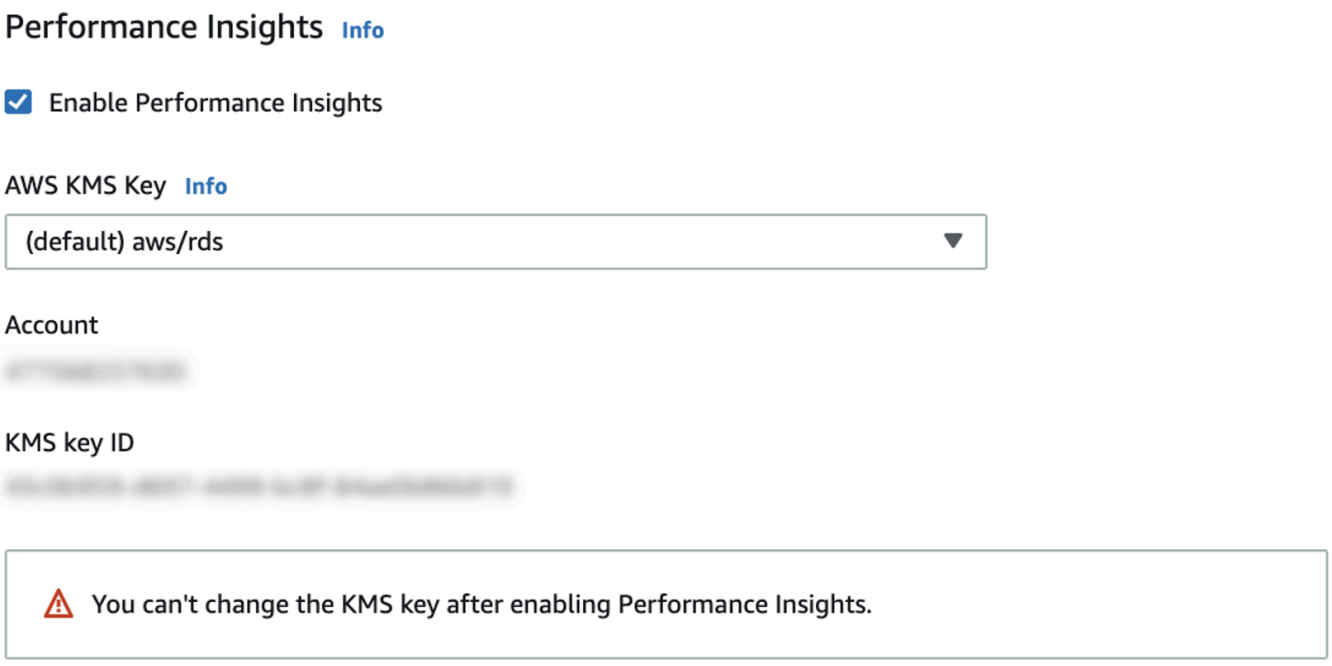
En la consola, puede activar o desactivar Información sobre rendimiento al crear o modificar una nueva instancia de base de datos.

Utilización del Consola de administración de AWS

En la consola, puede activar o desactivar Información sobre rendimiento al crear un clúster de Amazon DocumentDB. Cuando cree un nuevo clúster de Amazon DocumentDB, active Información sobre rendimiento con la opción Habilitar Información sobre rendimiento de la sección Información sobre rendimiento.

Instrucciones de la consola

1. Para crear un clúster, siga las instrucciones para Creación de un clúster de base de datos de Amazon DocumentDB.
2. En la sección Información sobre rendimiento, elija Activar Información sobre rendimiento.



> **Note**
>
> El período de retención de datos de Información sobre rendimiento será de siete días.

AWS KMS clave: especifique su clave AWS KMS. Performance Insights cifra todos los datos potencialmente confidenciales con su AWS KMS clave. Las datos se cifran en reposo y en tránsito. Para obtener más información, consulte Configuración de una AWS AWS KMS política para Performance Insights.

Activación y desactivación al modificar una instancia

Puede modificar una instancia de base de datos para habilitar Información sobre rendimiento mediante la consola o la AWS CLI.

Using the Consola de administración de AWS

Instrucciones de la consola

1. Inicie sesión en y abra la Consola de administración de AWS consola de Amazon DocumentDB en https://console.aws.amazon.com /docdb.
2. Seleccione Clusters (Clústeres).
3. Seleccione una instancia de base de datos y elija Modificar.
4. En la sección Información sobre rendimiento, elija Activar Información sobre rendimiento o Desactivar Información sobre rendimiento.

   > **Note**
   >
   > Si elige Activar Performance Insights, puede especificar su AWS AWS KMS clave. Performance Insights cifra todos los datos potencialmente confidenciales con su AWS KMS clave. Las datos se cifran en reposo y en tránsito. Para obtener más información, consulte Cifrado de datos de Amazon DocumentDB en reposo.

5. Elija Continuar.

6. En Programación de modificaciones, elija Aplicar inmediatamente. Si elige Aplicar durante la próxima ventana de mantenimiento programada, la instancia ignora esta configuración y habilita de inmediato Información sobre rendimiento.
7. Elija Modificar instancia.

Using the AWS CLI

Al usar los `modify-db-instance` AWS AWS CLI comandos `create-db-instance` o, puede habilitar Performance Insights especificando `--enable-performance-insights` o deshabilitarlo especificando`--no-enable-performance-insights`.

En el siguiente procedimiento, se describe cómo se activa o desactiva Información sobre rendimiento en una instancia de base de datos a través de AWS AWS CLI.

AWS AWS CLI instrucciones

Llame al `modify-db-instance` AWS AWS CLI comando y proporcione los siguientes valores:

- `--db-instance-identifer`: nombre de la instancia de la base de datos.
- `--enable-performance-insights` para activarlo o `--no-enable-performance-insights` para desactivarlo.

Example

El siguiente ejemplo habilita Información sobre rendimiento para `sample-db-instance`:

For Linux, macOS, or Unix:

```
aws docdb modify-db-instance \
    --db-instance-identifier sample-db-instance \
    --enable-performance-insights
```

For Windows:

```
aws docdb modify-db-instance ^
    --db-instance-identifier sample-db-instance ^
    --enable-performance-insights
```

Configuración de directivas de acceso para información sobre rendimiento

Para acceder a Información sobre rendimiento, debe tener los permisos adecuados de AWS Identity and Access Management (IAM). Tiene las siguientes opciones para conceder acceso:

- Asocie la política administrada `AmazonRDSPerformanceInsightsReadOnly` a un conjunto de permisos o a un rol.
- Cree una política de IAM personalizada y asóciela a un conjunto de permisos o a un rol.

Además, si especificó una clave administrada por el cliente al activar Información sobre rendimiento, asegúrese de que los usuarios de su cuenta tengan los permisos `kms:Decrypt` y `kms:GenerateDataKey` sobre la clave de KMS.

> **Note**
>
> Para la encryption-at-rest administración de AWS KMS claves y grupos de seguridad, Amazon DocumentDB aprovecha la tecnología operativa que se comparte con Amazon RDS.

Adjuntar la RDSPerformance InsightsReadOnly política de Amazon a un director de IAM

`AmazonRDSPerformanceInsightsReadOnly`es una política AWS gestionada que concede acceso a todas las operaciones de solo lectura de la API Performance Insights de Amazon DocumentDB. Actualmente, todas las operaciones de esta API son de solo lectura. Si asocia `AmazonRDSPerformanceInsightsReadOnly` a un conjunto de permisos o a un rol, el destinatario puede utilizar Información de rendimiento con las demás características de la consola.

Creación de una política de IAM personalizada para la información sobre rendimiento

Para los usuarios que no tienen la política `AmazonRDSPerformanceInsightsReadOnly`, puede conceder acceso a Información sobre rendimiento creando o modificando una política de IAM administrada por el usuario. Al asociar la política a un conjunto de permisos o a un rol, el destinatario puede utilizar Información de rendimiento.

Creación de una política personalizada

1. Abra la consola de IAM en https://console.aws.amazon.com/iam/.

2. En el panel de navegación, seleccione Políticas.
3. Elija Create Policy (Crear política).
4. En la página Create Policy (Crear política), elija la pestaña JSON.
5. Copie y pegue el siguiente texto y *us-east-1* sustitúyalo por el nombre de su AWS región y su número de cuenta de *111122223333* cliente.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "rds:DescribeDBInstances",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "rds:DescribeDBClusters",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "pi:DescribeDimensionKeys",
            "Resource": "arn:aws:pi:us-east-1:111122223333:metrics/rds/*"
        },
        {
            "Effect": "Allow",
            "Action": "pi:GetDimensionKeyDetails",
            "Resource": "arn:aws:pi:us-east-1:111122223333:metrics/rds/*"
        },
        {
            "Effect": "Allow",
            "Action": "pi:GetResourceMetadata",
            "Resource": "arn:aws:pi:us-east-1:111122223333:metrics/rds/*"
        },
        {
            "Effect": "Allow",
            "Action": "pi:GetResourceMetrics",
            "Resource": "arn:aws:pi:us-east-1:111122223333:metrics/rds/*"
```

```
        },
        {
            "Effect": "Allow",
            "Action": "pi:ListAvailableResourceDimensions",
            "Resource": "arn:aws:pi:us-east-1:111122223333:metrics/rds/*"
        },
        {
            "Effect": "Allow",
            "Action": "pi:ListAvailableResourceMetrics",
            "Resource": "arn:aws:pi:us-east-1:111122223333:metrics/rds/*"
        }
    ]
}
```

6. Elija Review policy (Revisar política).
7. Proporcione un nombre para la política y, opcionalmente, una descripción, a continuación, elija Create policy (Crear política).

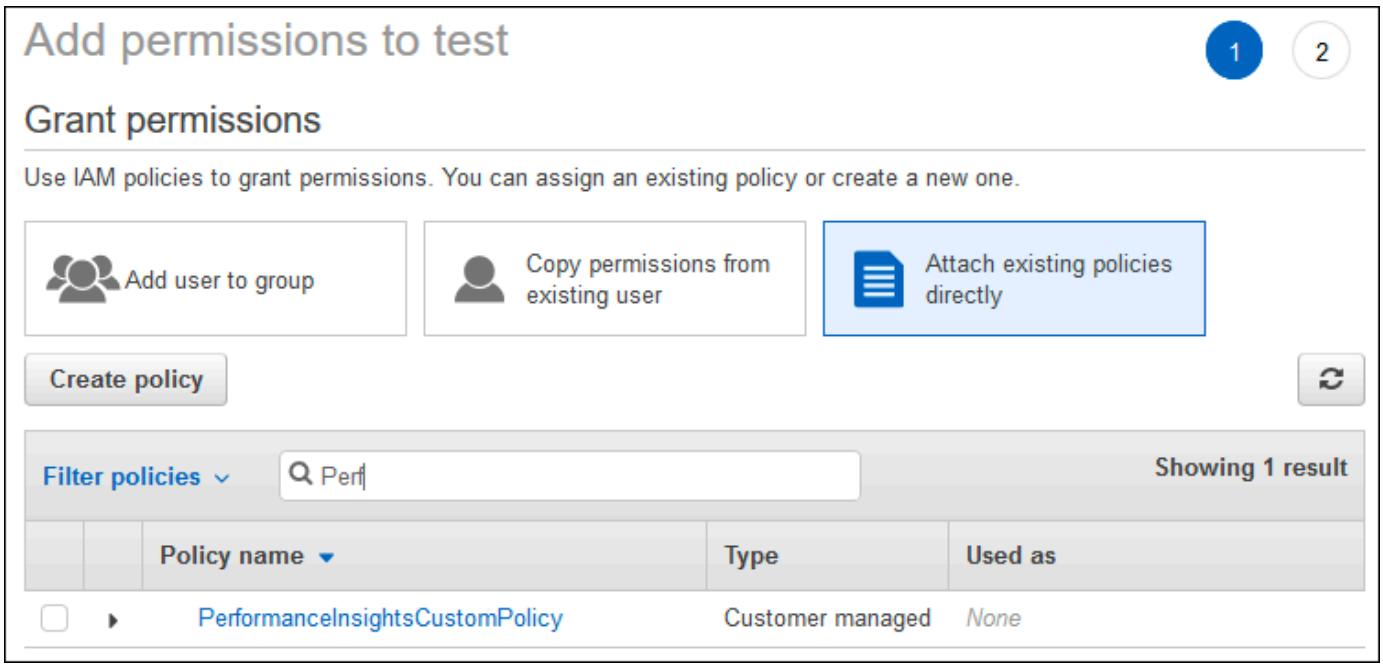
Ahora ya puede asociar la política a un conjunto de permisos o a un rol. En el procedimiento siguiente, se presupone que ya tiene un usuario para este fin.

Asociación de la política a un usuario

1. Abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. En el panel de navegación, seleccione Users.
3. Elija en la lista un usuario existente.

> **Important**
>
> Para utilizar Información sobre rendimiento, asegúrese de tener acceso a Amazon DocumentDB además de la política personalizada. Por ejemplo, la política AmazonDocDBReadOnlyAccesspredefinida proporciona acceso de solo lectura a Amazon DocDB. Para obtener más información, consulte Administrar el acceso mediante políticas.

4. En la página Resumen, elija Añadir permisos.
5. Elija Attach existing policies directly (Adjuntar políticas existentes directamente). En Search (Buscar), escriba los primeros caracteres del nombre de la política, como se muestra más abajo.



6. Elija la política y, a continuación, elija Next: Review.
7. Elija Add permissions (Agregar permisos).

Configuración de una AWS KMS política para Performance Insights

Performance Insights utiliza AWS KMS key y para cifrar datos confidenciales. Cuando habilita la información sobre rendimiento a través de la API o la consola, tiene las siguientes opciones:

- Elija la opción predeterminada Clave administrada de AWS.

  Amazon DocumentDB usa el Clave administrada de AWS para su nueva instancia de base de datos. Amazon DocumentDB crea una Clave administrada de AWS para su cuenta. AWS Su AWS cuenta tiene una cuenta de Amazon DocumentDB diferente Clave administrada de AWS para cada AWS región.
- Elija una clave administrada por el cliente.

  Si especifica una clave administrada por el cliente, los usuarios de su cuenta que llamen a la API de Performance Insights necesitarán los permisos `kms:Decrypt` y `kms:GenerateDataKey` sobre la clave de KMS. Puede configurar estos permisos a través de directivas de IAM. Sin embargo, le recomendamos que administre estos permisos a través de su directiva de clave KMS. Para obtener más información, consulte Uso de políticas clave en AWS KMS.

Example

La siguiente política de clave de ejemplo muestra cómo agregar instrucciones a la clave de KMS. Estas instrucciones permiten el acceso a la información sobre rendimiento. En función de cómo la utilice AWS KMS, es posible que desee cambiar algunas restricciones. Antes de agregar sentencias a la directiva, elimine todos los comentarios.

Análisis de métricas mediante el panel de Información sobre rendimiento

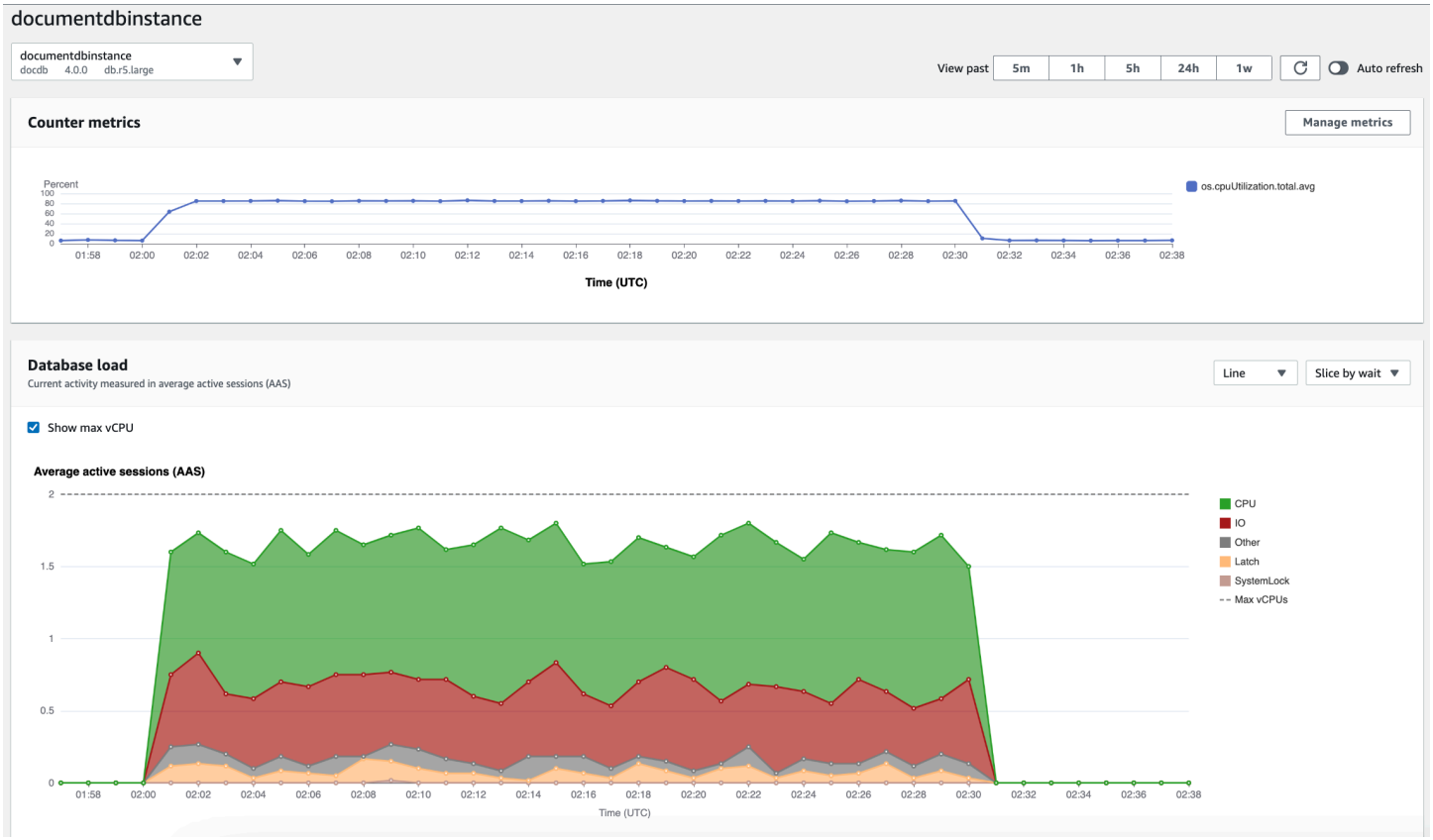
El panel de Información sobre rendimiento contiene información de desempeño de la base de datos para ayudarle a analizar y solucionar los problemas de desempeño. En la página del panel principal, encontrará información sobre la carga de la base de datos (DB load). Puede “dividir” la carga de la base de datos por dimensiones, como eventos de espera o de consulta.

Temas

- Información general del panel de Información sobre rendimiento
- Apertura del panel de Información sobre rendimiento
- Análisis de carga de la base de datos mediante estados de espera
- Información general sobre la pestaña Top queries
- Ampliación del gráfico de carga de base de datos

Información general del panel de Información sobre rendimiento

El panel es la forma más sencilla de interactuar con Información sobre rendimiento. El siguiente ejemplo muestra el panel de una instancia de Amazon DocumentDB. De forma predeterminada, el panel de Información sobre rendimiento muestra los datos de la última hora.



El panel está dividido en las partes siguientes:

1. Métricas de contador: muestra los datos para métricas de contador de rendimiento específicas.
2. Gráfico de carga de base de datos: muestra cómo se compara la carga de base de datos con la capacidad de instancia de base de datos representada por la línea de vCPU máximas.
3. Principales dimensiones: muestra las dimensiones principales que contribuyen a la carga de la base de datos. Estas dimensiones incluyen `waits`, `queries`, `hosts`, `databases` y `applications`.

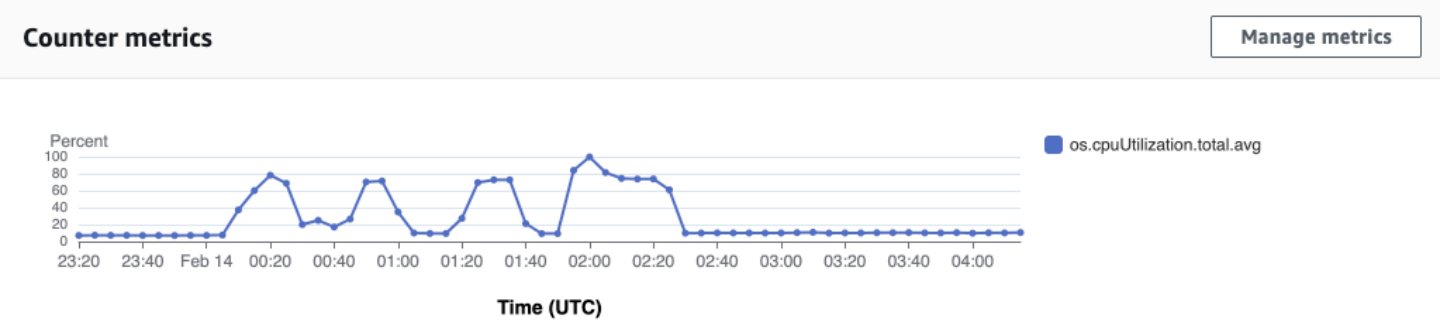
Temas

- Gráfico Counter metrics (Métricas de contador)
- Gráfico Database load (Carga de base de datos)
- Tabla de dimensiones principales

Gráfico Counter metrics (Métricas de contador)

Con las métricas de contador, puede personalizar el panel de Información sobre rendimiento para que incluya hasta 10 gráficos adicionales. Estos gráficos muestran una selección de docenas de métricas de rendimiento de sistemas operativos y bases de datos. Esta información se puede correlacionar con la carga de base de datos para ayudar a identificar y analizar problemas de rendimiento.

El gráfico Counter metrics (Métricas de contador) muestra los datos para los contadores de rendimiento.



Para cambiar los contadores de rendimiento, elija Administrar métricas. Puede seleccionar varias métricas del sistema operativo como se muestra en la siguiente captura de pantalla. Para ver los detalles de cualquier métrica, sitúe el cursor sobre el nombre de la métrica.

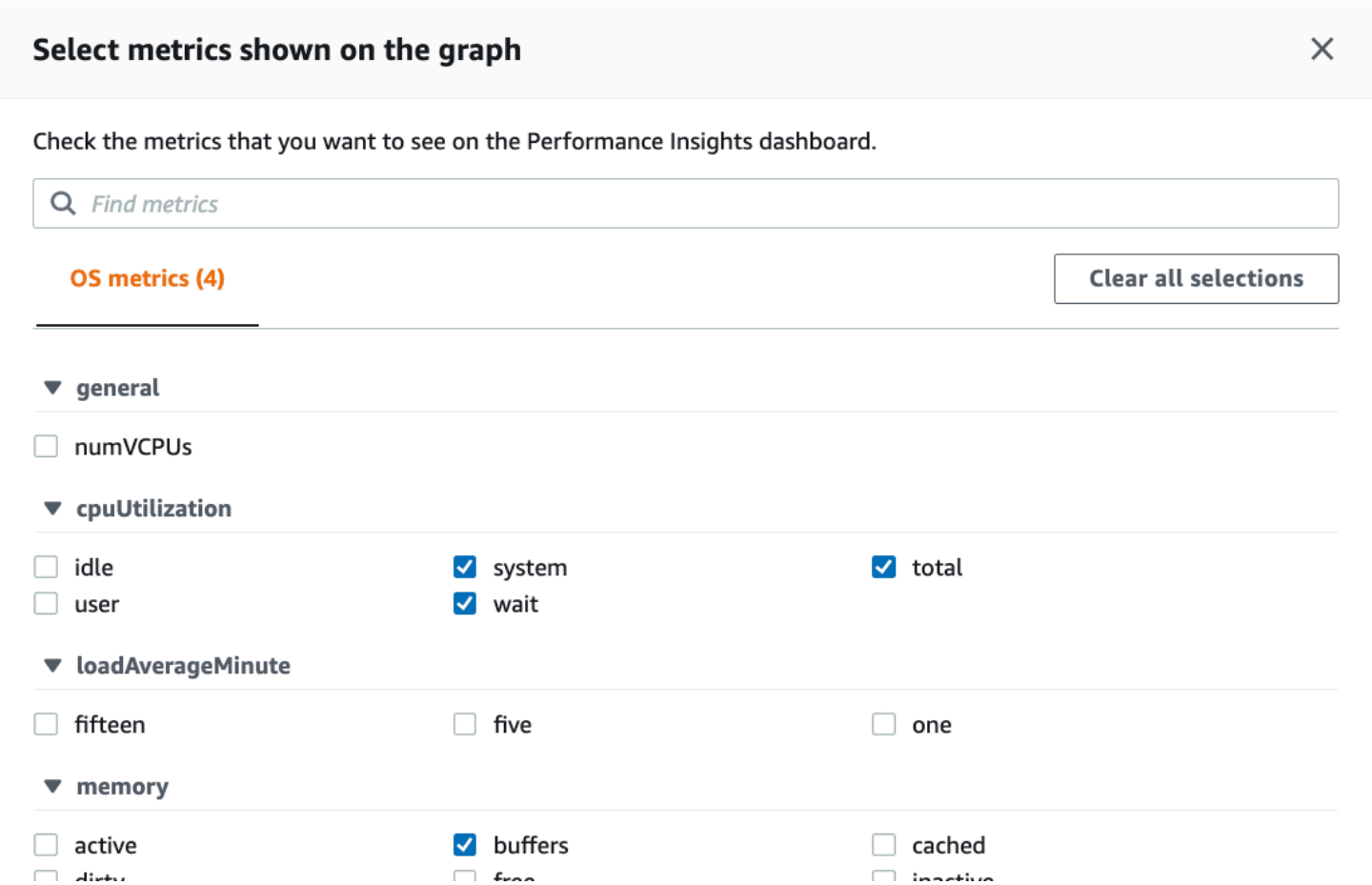


Gráfico Database load (Carga de base de datos)

El gráfico Carga de base de datos muestra cómo se compara la carga de base de datos con la capacidad de la instancia de base de datos representada por la línea Max vCPU (Máximo de vCPU). De forma predeterminada, el gráfico de líneas apilado representa la carga de base de datos como promedio de sesiones activas por unidad de tiempo. La carga de base de datos está dividida (agrupada) por estados de espera.



Carga de base de datos dividida por dimensiones

Puede elegir ver la carga como sesiones activas agrupadas por cualquier dimensión admitida. En la imagen siguiente, se muestran las dimensiones de una instancia de Amazon DocumentDB.



Detalles de carga de base de datos de un elemento de dimensión

Para consultar los detalles de un elemento de carga de base de datos dentro de una dimensión, pase el cursor sobre el nombre de elemento. En la imagen siguiente, se muestran los detalles de una instrucción de consulta.



Para consultar los detalles de cualquier elemento para el periodo de tiempo seleccionado en la leyenda, coloque el cursor sobre ese elemento.

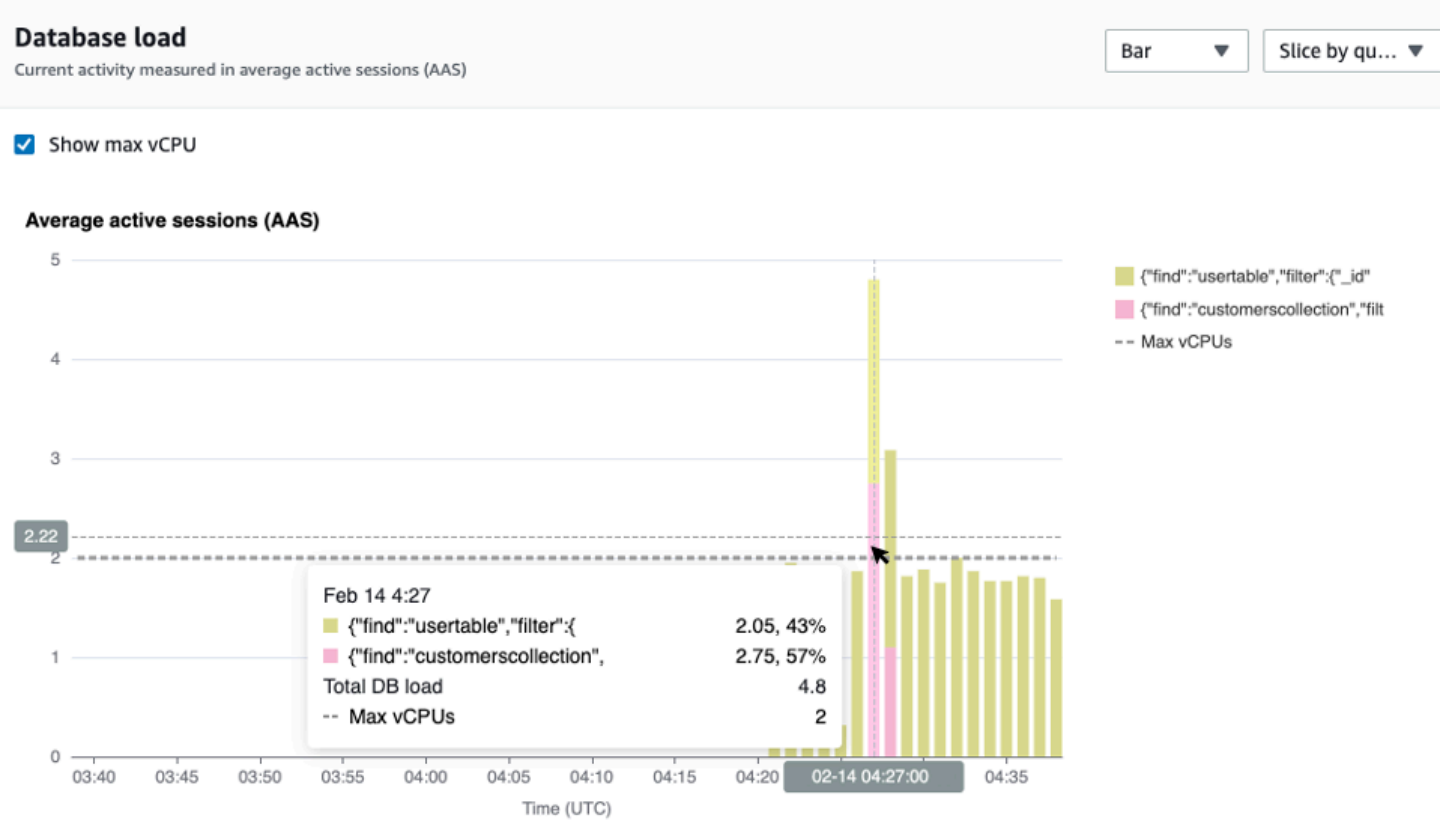
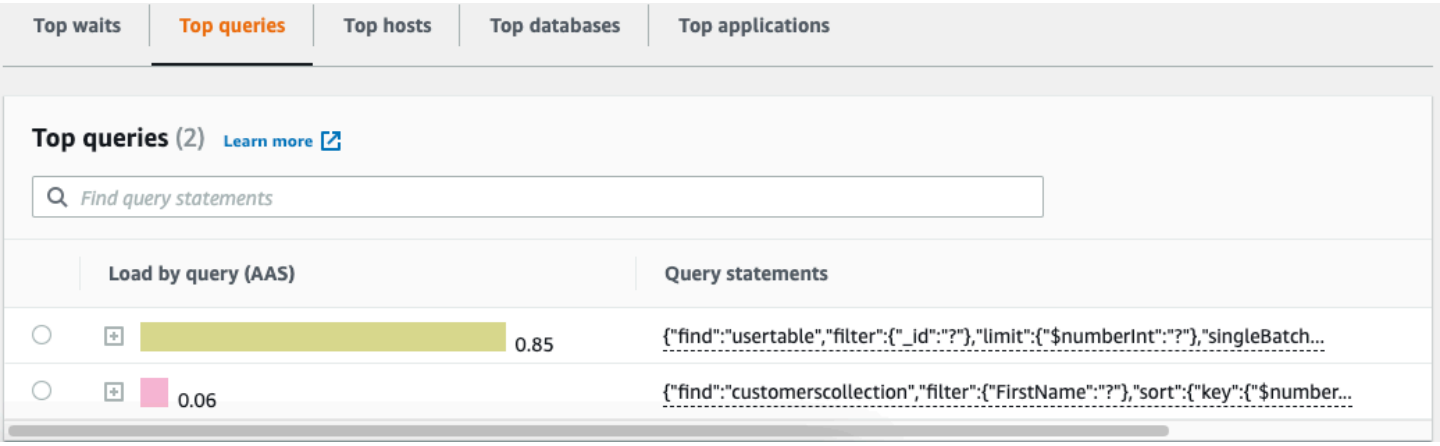


Tabla de dimensiones principales

La tabla de dimensiones principales divide la carga de base de datos por diferentes dimensiones. Una dimensión es una categoría o “dividir por” para diferentes características de la carga de base de datos. Si la dimensión es consulta, Consultas principales muestra las instrucciones de consulta que más contribuyen a la carga de bases de datos.

Elija cualquiera de las siguientes pestañas de dimensión.



En la siguiente tabla, se proporciona una breve descripción de cada pestaña.

Detalles	Descripción
Esperas principales por	El evento por el que la base de datos de backend está esperando.
Consultas principales	Las instrucciones de consulta que se están ejecutando
Hosts principales	El host y el puerto

Dimensión (Descripción)	Descripción
Base de datos	El nombre de la base de datos principal a la que está conectado el cliente.
del cliente conectado	

Description (Descripción)
Aplicaciones principales: el nombre de la aplicación que está conectada a la base de datos.

Para obtener más información sobre cómo analizar las consultas mediante la pestaña Consulta principal, consulte Información general sobre la pestaña Top queries.

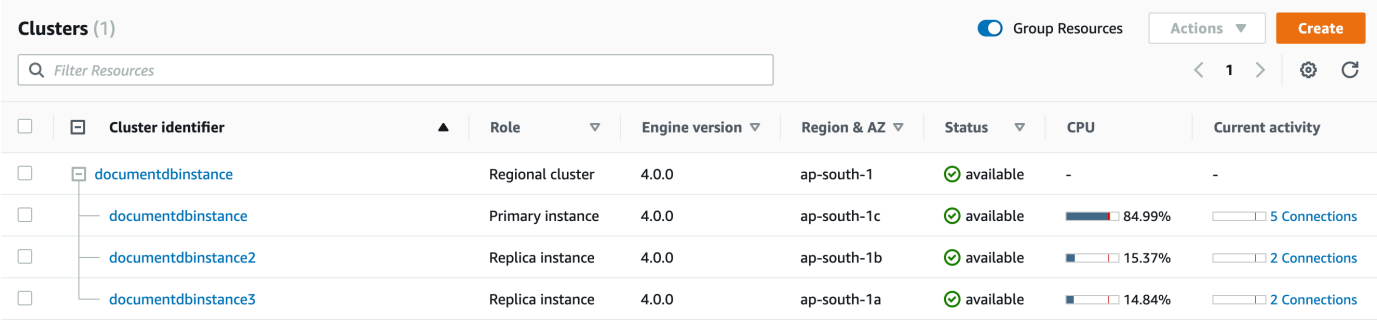
Apertura del panel de Información sobre rendimiento

Para ver el panel de Performance Insights en la consola de AWS administración, siga estos pasos:

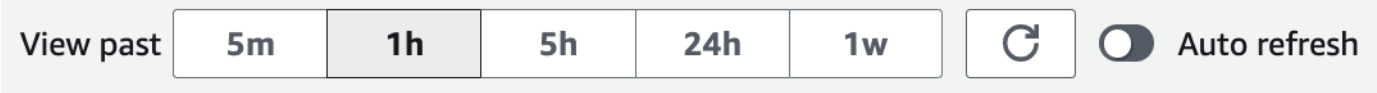
1. Abra la consola Performance Insights en https://console.aws.amazon.com/docdb/.
2. Elija una instancia de base de datos. Se muestra el panel de Información sobre rendimiento para esa instancia de Amazon DocumentDB.

   En instancias de Amazon DocumentDB con Información sobre rendimiento habilitado, también puede acceder al panel eligiendo el elemento Sesiones en la lista de instancias de base de datos. En Actividad actual, el elemento Sesiones muestra la carga de la base de datos en el como promedio de sesiones activas en los últimos cinco minutos. La barra muestra gráficamente la carga. Cuando la barra está vacía, la instancia está inactiva. Conforme aumenta la carga, la

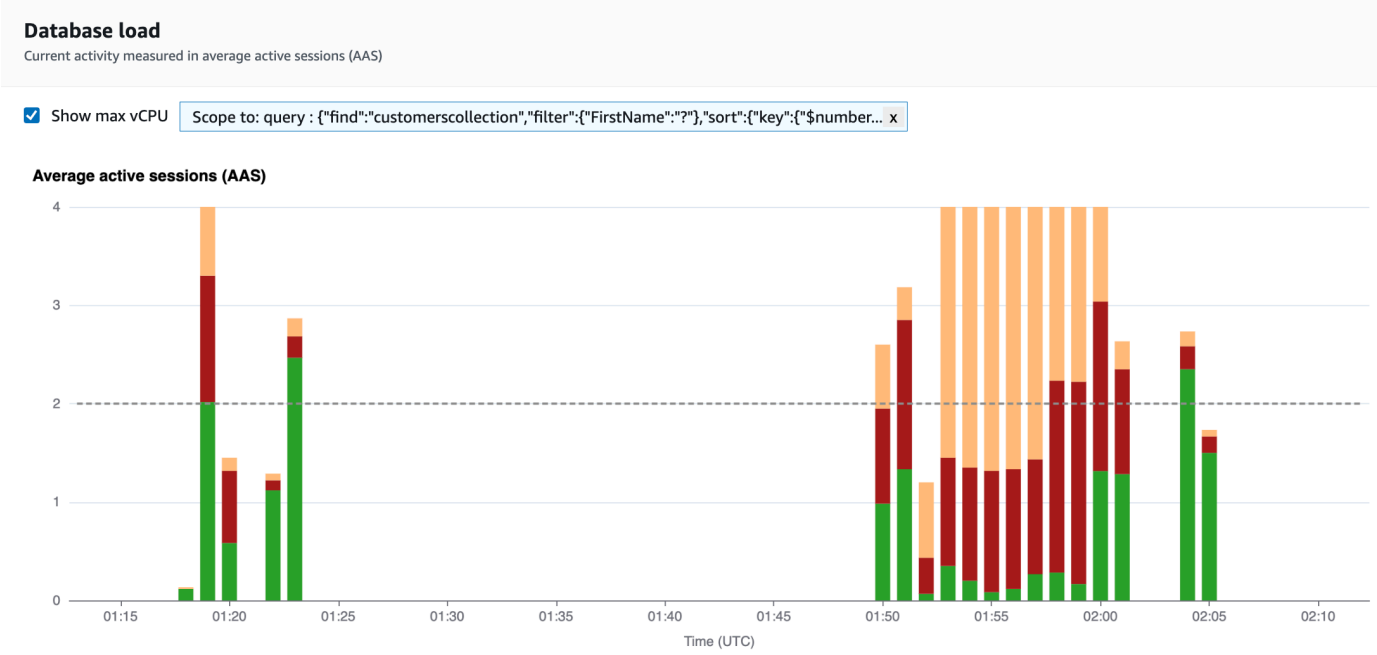
barra se va completando en azul. Cuando la carga supera el número de virtuales CPUs (vCPUs) de la clase de instancia, la barra se pone roja, lo que indica un posible cuello de botella.



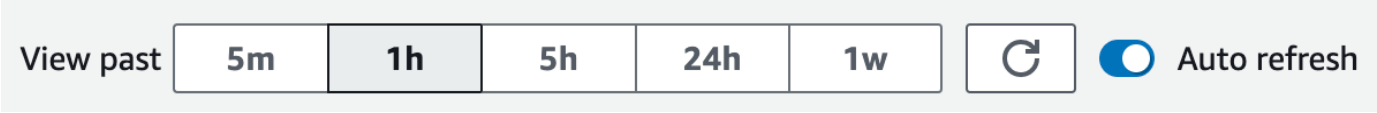
3. (Opcional) Elija un intervalo de tiempo diferente seleccionando un botón en la parte superior derecha. Por ejemplo, para cambiar el intervalo a 1 horas, seleccione 1h.



En la siguiente captura de pantalla, el intervalo de carga de la base de datos es de 1 horas.



4. Para actualizar los datos automáticamente, habilite Actualización automática.



El panel de información sobre rendimiento se actualiza automáticamente con nuevos datos. La frecuencia de actualización depende de la cantidad de datos mostrados:

- 5 minutos actualiza cada 5 segundos.
- 1 hora actualiza cada minuto.
- 5 horas actualiza cada minuto.
- 24 horas actualiza cada 5 minutos.
- 1 semana actualiza cada hora.

Análisis de carga de la base de datos mediante estados de espera

Si el gráfico Carga de base de datos indica que hay un cuello de botella, puede averiguar de dónde procede la carga. Para ello, fíjese en la tabla de elementos de carga principales situada debajo del gráfico Carga de base de datos. Elija un elemento en particular, como una consulta o un usuario, para ampliar la información de ese elemento y ver los detalles.

La carga de base de datos agrupada por esperas y principales consultas normalmente ofrece la máxima información sobre problemas de rendimiento. La carga de la base de datos agrupada por esperas indica si hay algún cuello de botella de simultaneidad o recursos en la base de datos. En este caso, la pestaña Consultas principales de la tabla de elementos de carga principales indica qué consultas están contribuyendo a esa carga.

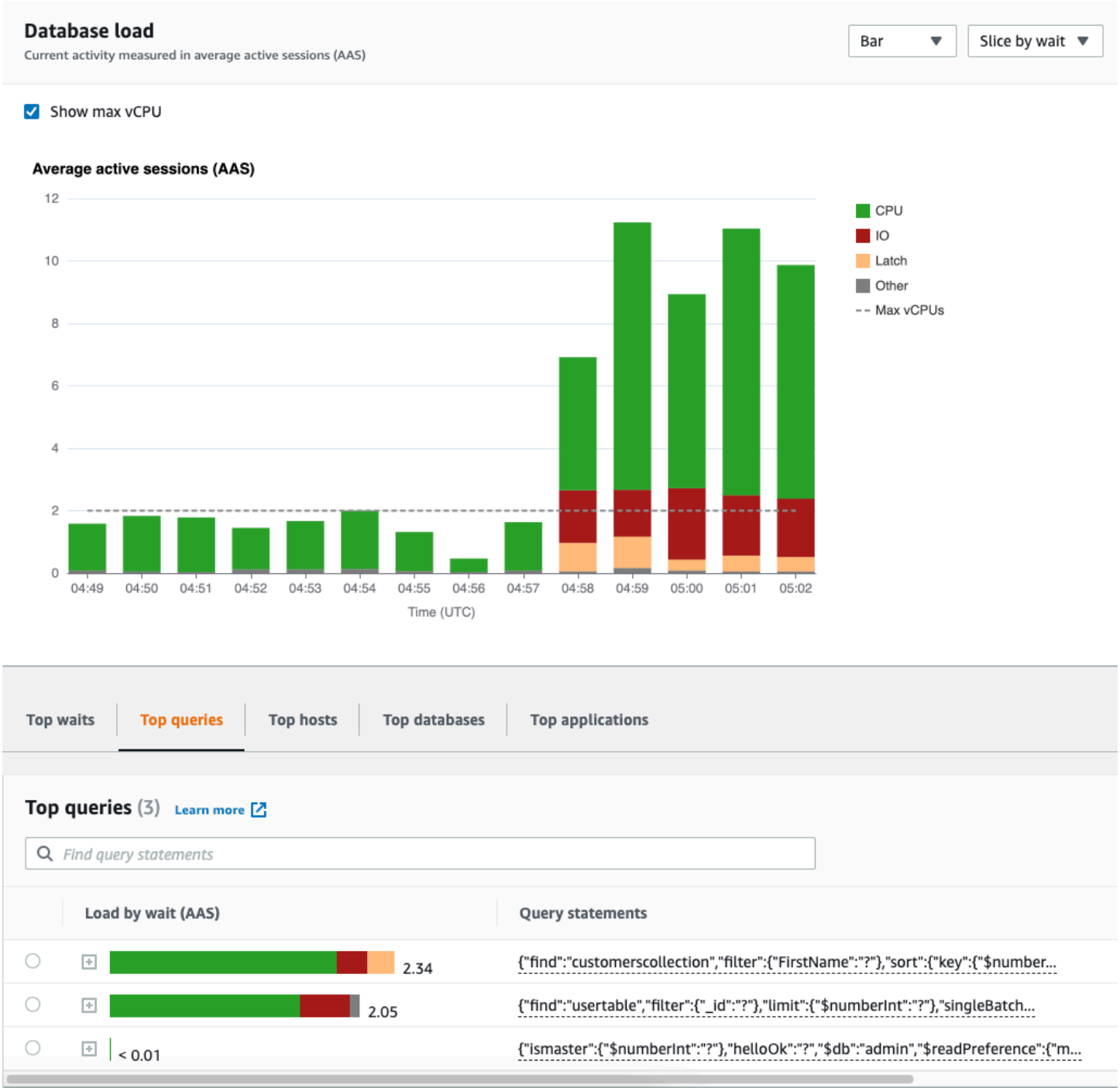
Este es el flujo de trabajo típico para diagnosticar los problemas de desempeño:

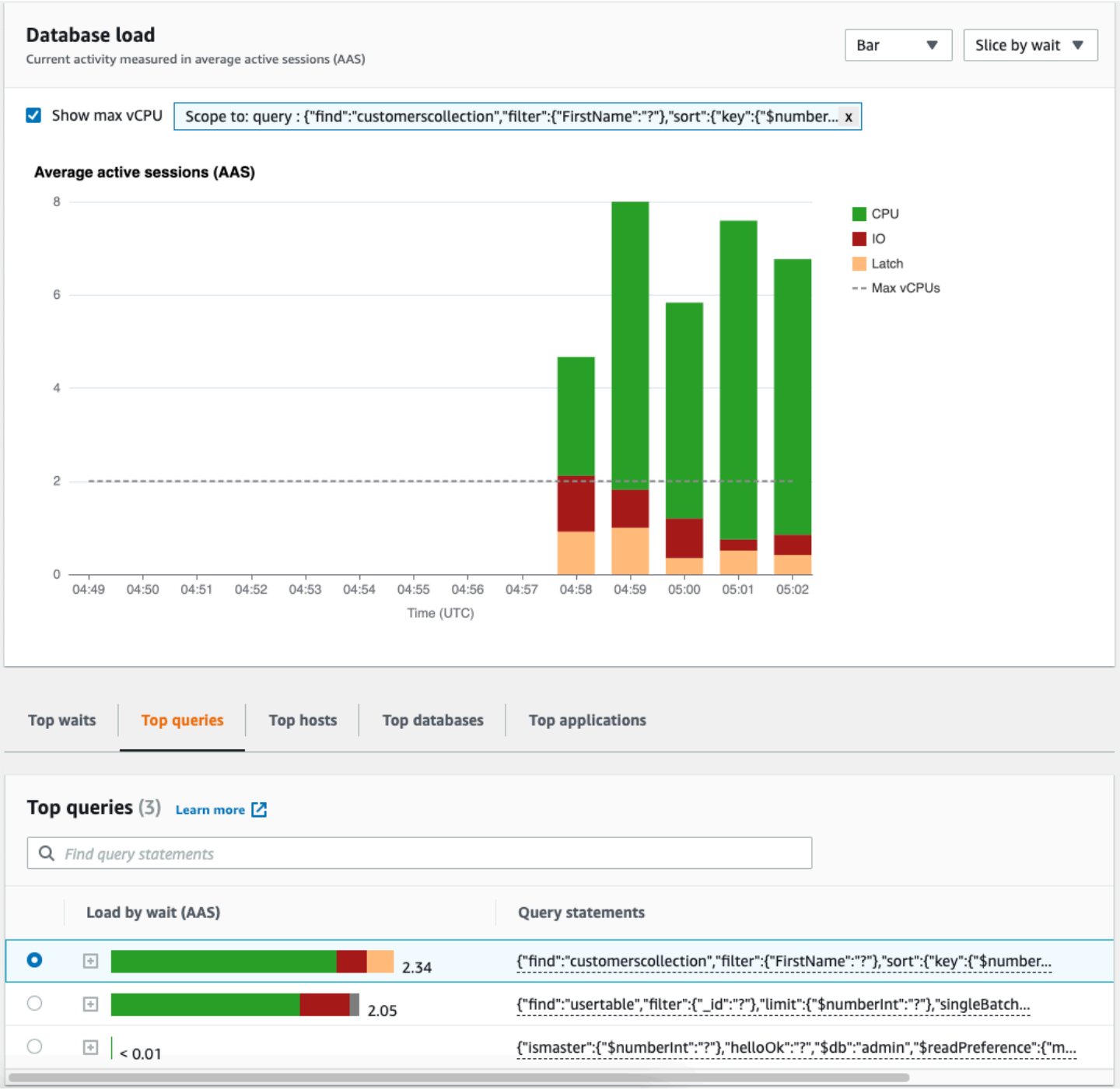
1. Revise el gráfico Carga de base de datos para ver si hay algún incidente de carga de base de datos que sobrepase la línea Máximo de CPU.
2. De ser así, fíjese en el gráfico Carga de base de datos e identifique qué estado o estados de espera son los principales responsables.
3. Para identificar las consultas de resumen que están provocando la carga, consulte qué consultas de la pestaña Top queries de la tabla de elementos de carga principales están contribuyendo más a esos estados de espera. Para identificarlas, utilice la columna Carga de base de datos por espera.
4. Elija una de estas consultas de resumen en la pestaña Top queries para ampliarla y ver las consultas secundarias que contiene.

También puede ver qué hosts o aplicaciones generan más carga seleccionando los Alojamientos principales o Aplicaciones principales, respectivamente. Los nombres de las aplicaciones se

especifican en la cadena de conexión a la instancia de Amazon DocumentDB. Unknown indica que no se especificó el campo de la aplicación.

Por ejemplo, en el panel que se muestra a continuación, la espera de la sincronización de archivos de registro se corresponde con la mayor parte de la carga de base de datos. Al seleccionar la consulta principal en Consultas principales, se analizará el diagrama de carga de la base de datos para centrarse en la mayor carga que aporta la consulta seleccionada.





Información general sobre la pestaña Top queries

De forma predeterminada, la pestaña Consultas principales muestra las consultas que más contribuyen a la carga de base de datos. Puede analizar el texto de la consulta para ajustarlas.

Temas

- Resúmenes de consultas

- Carga por esperas (AAS)
- Visualización de información detallada de la consulta
- Acceso al texto de consulta de la declaración
- Visualización y descarga del texto de consulta de la declaración

Resúmenes de consultas

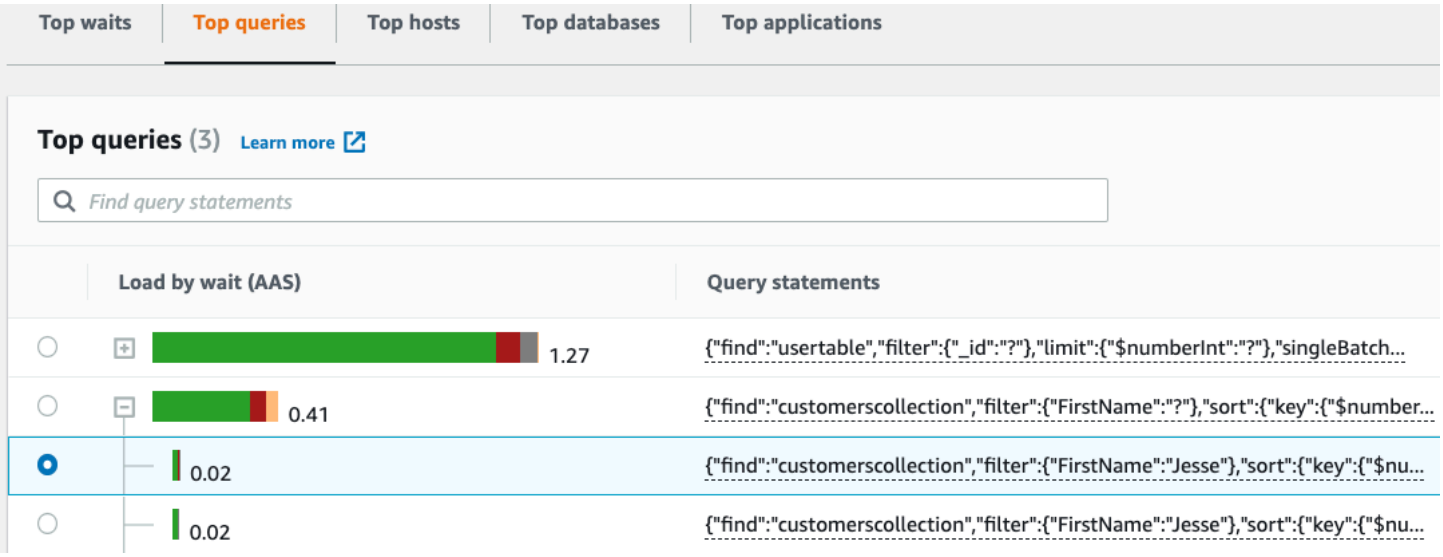
Un resumen de consultas es un compuesto de múltiples consultas reales que son similares en estructura, pero que pueden tener diferentes valores literales. El resumen reemplaza los valores codificados por un signo de interrogación. Por ejemplo, un resumen de una consulta podría verse de la siguiente manera:

```
{"find":"customerscollection","filter":{"FirstName":"?"},"sort":{"key":
{"$numberInt":"?"}},"limit":{"$numberInt":"?"}}
```

Este resumen podría incluir las siguientes consultas secundarias:

```
{"find":"customerscollection","filter":{"FirstName":"Karrie"},"sort":{"key":
{"$numberInt":"1"}},"limit":{"$numberInt":"3"}}
{"find":"customerscollection","filter":{"FirstName":"Met"},"sort":{"key":
{"$numberInt":"1"}},"limit":{"$numberInt":"3"}}
{"find":"customerscollection","filter":{"FirstName":"Rashin"},"sort":{"key":
{"$numberInt":"1"}},"limit":{"$numberInt":"3"}}
```

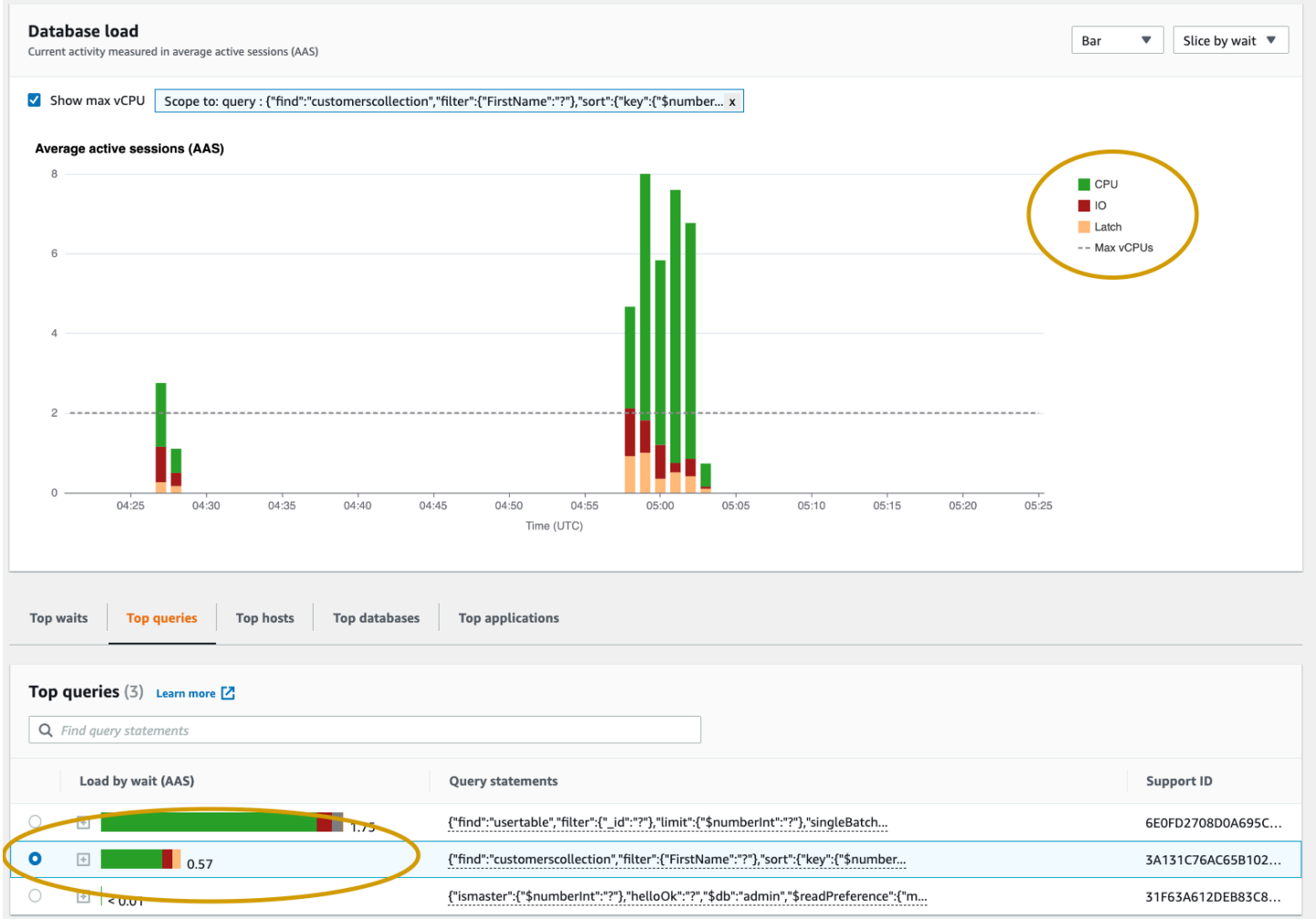
Para ver las instrucciones de consulta literales de un resumen, seleccione la consulta y, a continuación, elija el símbolo más (+). En la siguiente captura de pantalla, la consulta seleccionada es un resumen.



> **Note**
>
> Un resumen de consultas agrupa sentencias de consulta similares, pero no redacta información confidencial.

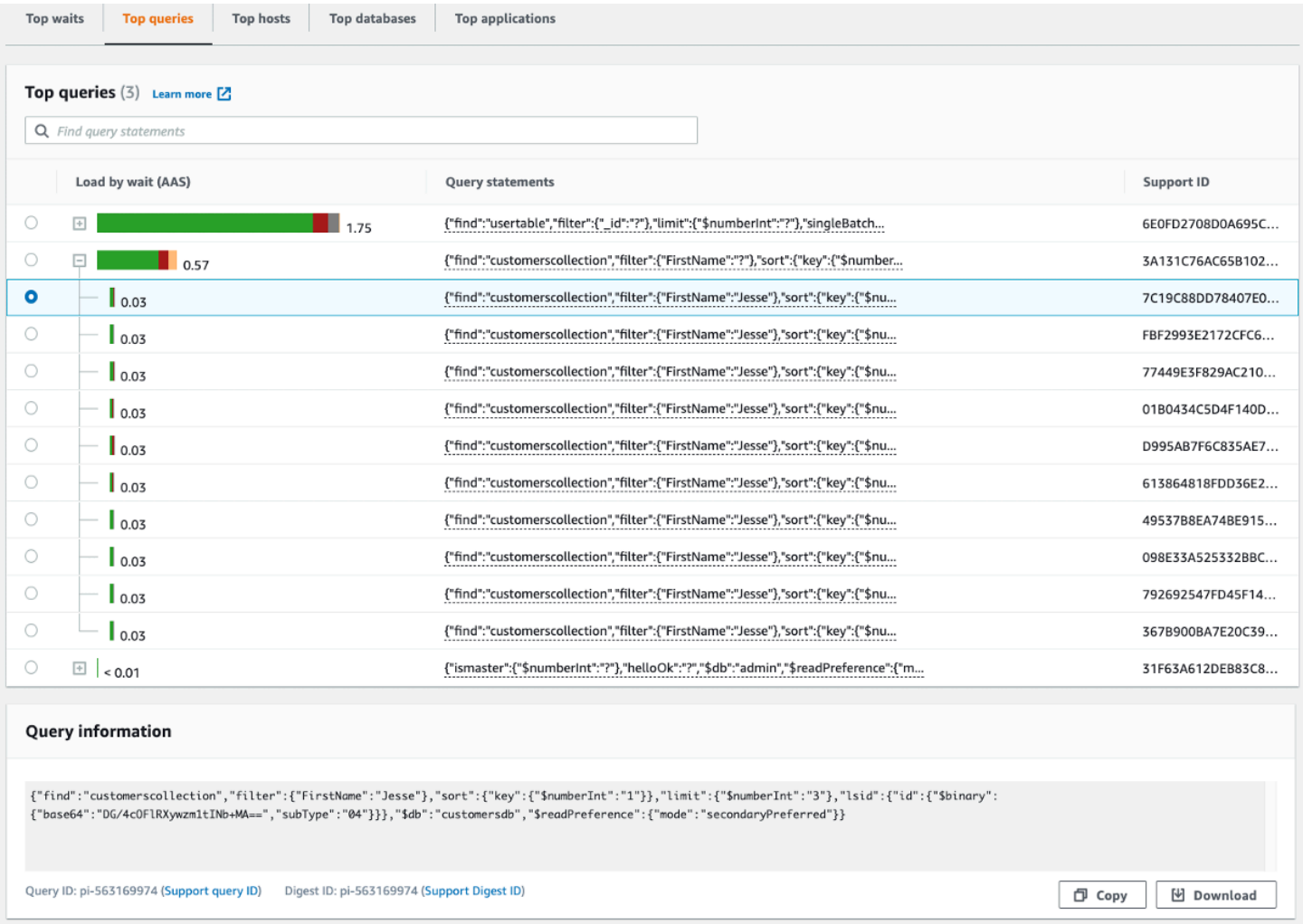
Carga por esperas (AAS)

En Consultas principales, la columna Carga por espera (AAS) ilustra el porcentaje de carga de la base de datos asociada con cada elemento de carga principal. Esta columna refleja la carga de ese elemento por cualquier agrupación que se haya seleccionado actualmente en el gráfico de carga de base de datos. Por ejemplo, es posible que pueda agrupar el gráfico DB load (Carga de base de datos) por estados de espera. En este caso, la barra DB Load by Waits (Carga de base de datos por esperas) estaría dimensionada, segmentada y dividida por colores para mostrar en qué proporción contribuye esa consulta a un estado de espera. También muestra qué estados de espera afectan a la consulta seleccionada.



Visualización de información detallada de la consulta

En la tabla Consulta principal, puede abrir un resumen de situación para consultar su información. La información aparece en el panel inferior.



Los siguientes tipos de identificadores (IDs) están asociados a las sentencias de consulta:

1. ID de consulta de soporte: un valor hash del ID de consulta. Este valor solo sirve para hacer referencia a un ID de consulta cuando se trabaja con AWS Support. AWS Support no tiene acceso a la consulta ni al texto IDs de la consulta reales.
2. Compatibilidad con ID de resumen: un valor hash del ID de resumen. Este valor solo sirve para hacer referencia a un ID de resumen cuando se trabaja con AWS Support. AWS Support no tiene acceso a tu resumen ni al texto IDs de consulta reales.

Acceso al texto de consulta de la declaración

De forma predeterminada, cada fila de la tabla Consultas principales muestra 500 bytes de texto para cada instrucción. Cuando una instrucción de consulta supera los 500 bytes, puede ver más texto abriendo la instrucción en el panel de Información sobre rendimiento. En este caso, la longitud

máxima de la consulta que se muestra es de 1 KB. Si ve una instrucción SQL secundaria, también puede elegir Descargar.

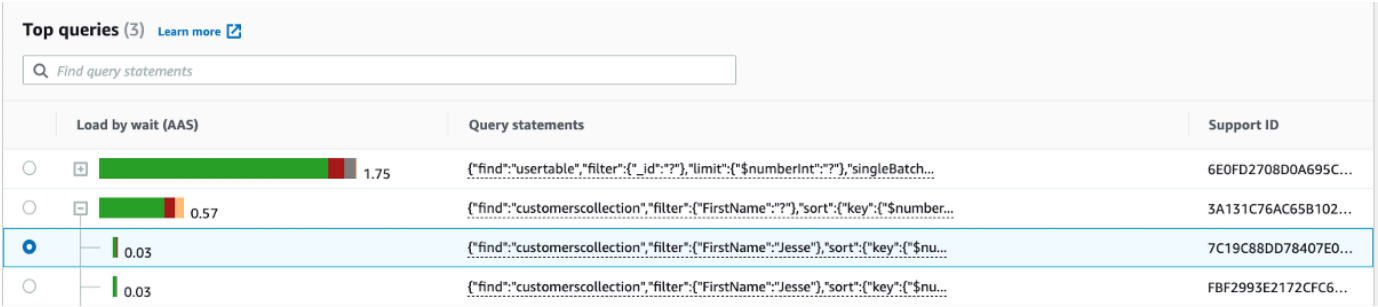
Visualización y descarga del texto de consulta de la declaración

Puede ver o descargar texto de consulta en el panel de Información sobre rendimiento.

Visualización de más texto de consulta en el panel de Información sobre rendimiento

1. Abra la consola de Amazon DocumentDB en: https://console.aws.amazon.com/docdb/
2. En el panel de navegación, seleccione Información sobre rendimiento.
3. Elija una instancia de base de datos. Se abre el panel de Información sobre rendimiento para esa instancia de base de datos.

   Las instrucciones de consulta con texto superior a 500 bytes son similares a las que se indican en la siguiente imagen.



4. Examine la sección de información de consulta para consultar más texto de consulta.



El panel de Información sobre rendimiento puede mostrar hasta 1 KB por cada instrucción de consulta completa.

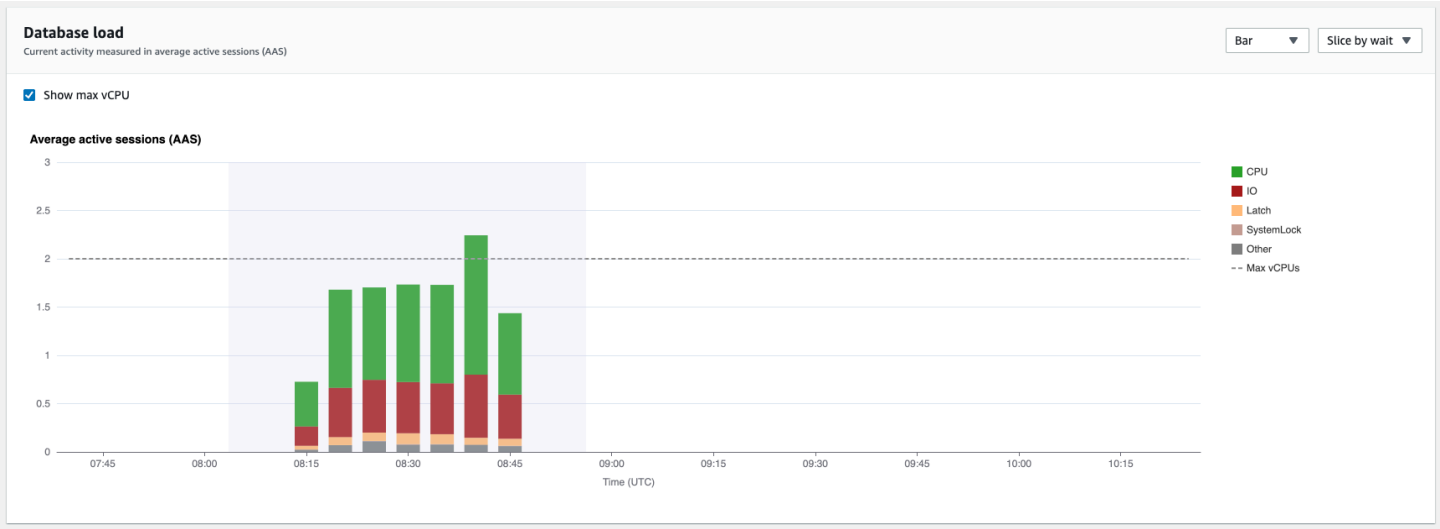
> **Note**
>
> Para copiar o descargar la instrucción de consulta, deshabilite los bloqueadores de pantallas emergentes.

Ampliación del gráfico de carga de base de datos

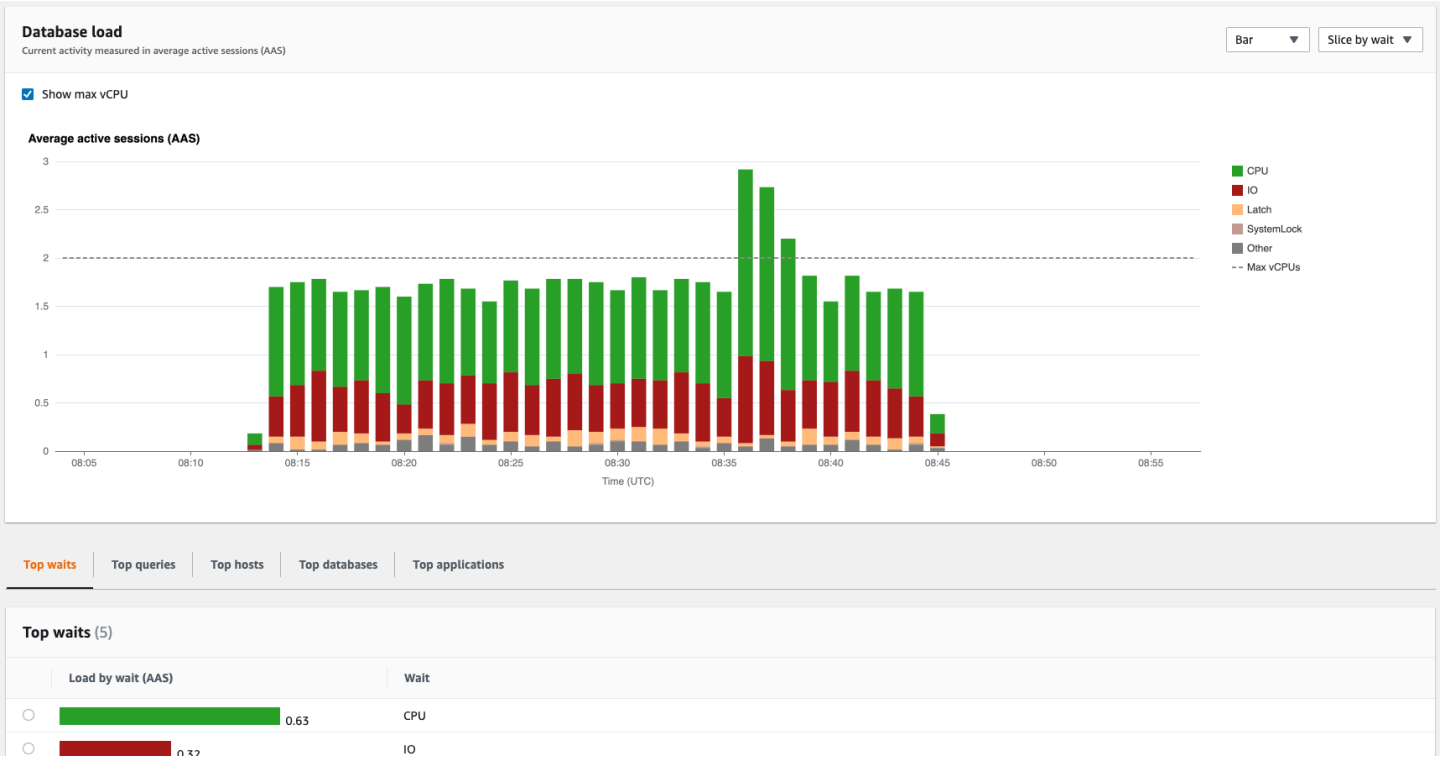
Hay otras características de la interfaz de usuario de Información sobre rendimiento que ayudan a analizar los datos de desempeño.

Click-and-Drag Ampliar

En la interfaz de Performance Insights, se puede seleccionar una pequeña parte del gráfico de carga y ampliarlo para ver los detalles.



Para ampliar una parte del gráfico de carga, elija la hora de inicio y arrastre el ratón hasta el final del período que desee. Al hacer esto, el área seleccionada queda resaltada. Cuando suelte el ratón, el gráfico de carga amplía el área seleccionada y se vuelve a calcular la tabla de Elementos principales.



Recuperación de métricas con la API de Información sobre rendimiento

Cuando se habilita Información sobre rendimiento, la API proporciona visibilidad sobre el rendimiento de la instancia. Amazon CloudWatch Logs proporciona la fuente autorizada de las métricas de monitoreo de los servicios de Vended. AWS

Con Performance Insights se ofrece una vista propia del dominio de la carga de la base de datos entendida como el promedio de sesiones activas (AAS). Esta métrica aparece para los consumidores de API como conjunto de datos de serie temporal bidimensional. La dimensión temporal de los datos ofrece datos de carga de base de datos para cada punto temporal del intervalo de tiempo consultado. Cada punto temporal descompone la carga global en relación con las dimensiones solicitadas, tales como `Query`, `Wait-state`, `Application` o `Host`, medidas en ese punto temporal.

Información sobre rendimiento de Amazon DocumentDB monitoriza la instancia de base de datos de Amazon DocumentDB para poder analizar y solucionar los problemas de desempeño de la base de datos. Una forma de ver los datos de Información sobre rendimiento es a través de la Consola de administración de AWS. Performance Insights además ofrece una API pública, para poder consultar en sus propios datos. Puede utilizar la API para hacer lo siguiente:

- Descarga de datos en una base de datos
- Agregación de datos de Performance Insights a los paneles de monitoreo existentes

- Creación de herramientas de monitoreo

Para utilizar la API de Información sobre rendimiento, habilite Información sobre rendimiento en una de sus instancias de base de datos de Amazon DocumentDB. Para obtener información sobre la habilitación de Información sobre rendimiento, consulte Activación y desactivación de Información sobre rendimiento. Para obtener información sobre la API de Información sobre rendimiento, consulte la Referencia de la API de Información sobre rendimiento.

La API de Información sobre rendimiento proporciona las siguientes operaciones.

Acción de Performance Insights	AWS CLI comando	Description (Descripción)
`DescribeDimensionKeys`	`aws pi describe-dimension-keys`	Recupera las principales claves de dimensión N de una métrica para un periodo de tiempo específico.
`GetDimensionKeyDetails`	`aws pi get-dimension-key-details`	Recupera los atributos del grupo de dimension es especificado para una instancia de base de datos o un origen de datos. Por ejemplo, si especifica un ID de consulta y si los detalles de la dimensión están disponibl es, `GetDimensionKeyDetails` recupera el texto completo de la dimensión `db.query.statement` asociada a este ID. Esta operación resulta útil porque `GetResourceMetrics` y `DescribeDimensionKeys` no admiten la recuperac ión de texto de instrucción de consulta grande.

Acción de Performance Insights	AWS CLI comando	Description (Descripción)
GetResourceMetadata	aws pi get-resource-metadata	Recupere los metadatos de las distintas características. Por ejemplo, los metadatos podrían indicar que una característica está activada o desactivada en una instancia de base de datos específica.
GetResourceMetrics	aws pi get-resource-metrics	Recupera las métricas de Información sobre rendimiento de un conjunto de orígenes de datos, durante un periodo de tiempo. Puede proporcionar grupos de dimensiones y dimensiones específicas, y proporcionar criterios de agregación y filtrado para cada grupo.
ListAvailableResourceDimensions	aws pi list-available-resource-dimensions	Recupere las dimensiones que se pueden consultar para cada tipo de métrica especificado en una instancia especificada.
ListAvailableResourceMetrics	aws pi list-available-resource-metrics	Recupere todas las métricas disponibles de los tipos de métricas especificados que se pueden consultar de una instancia de base de datos especificada.

Temas

- AWS CLI para Performance Insights
- Recuperación de métricas de series temporales
- AWS CLI ejemplos de Performance Insights

AWS CLI para Performance Insights

Puede ver los datos de Performance Insights a través de la AWS CLI. Puede obtener ayuda sobre los comandos de la AWS CLI de Performance Insights escribiendo lo siguiente en la línea de comandos.

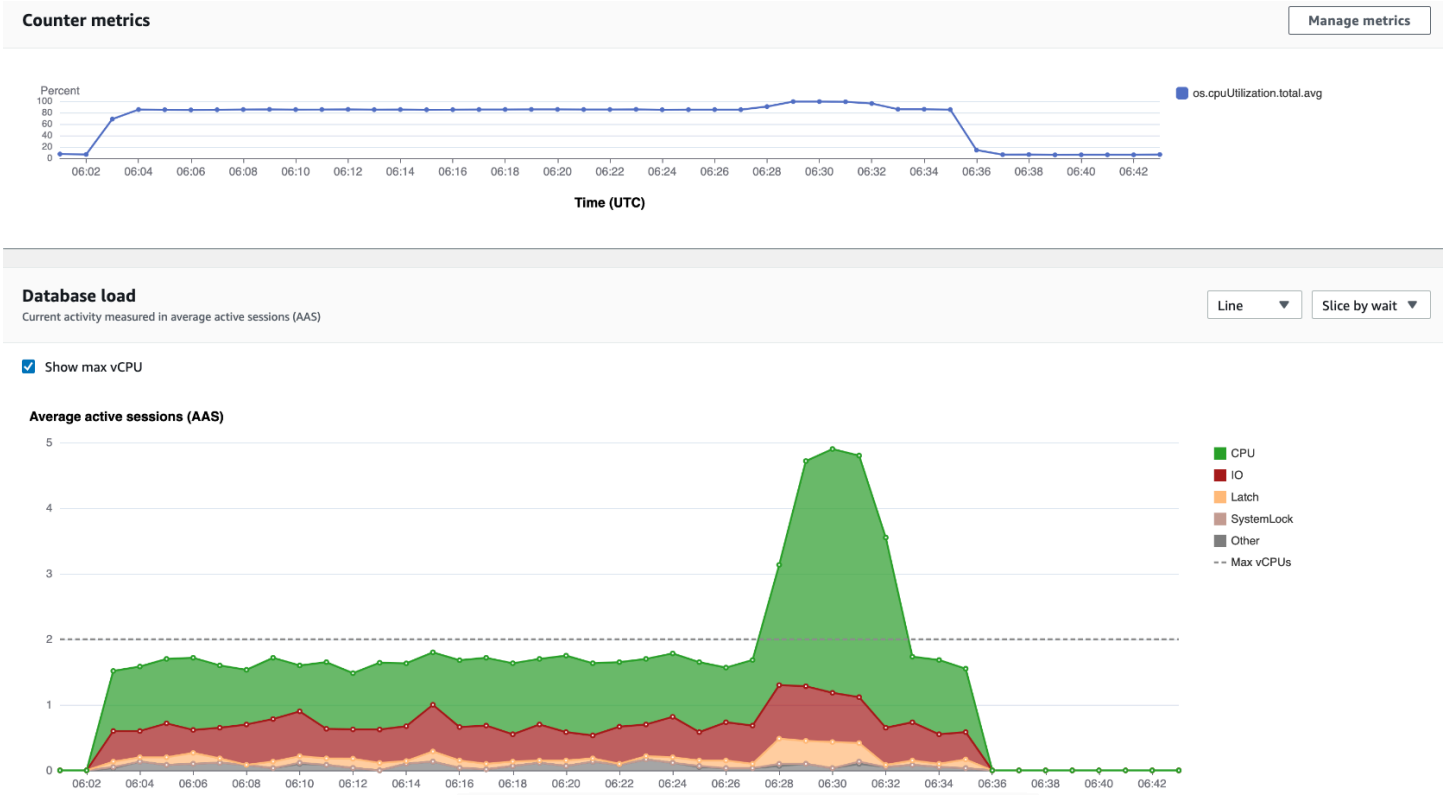
```
aws pi help
```

Si no la tiene AWS CLI instalada, consulte Instalación de la interfaz de línea de AWS comandos en la Guía del AWS CLI usuario para obtener información sobre cómo instalarla.

Recuperación de métricas de series temporales

La operación `GetResourceMetrics` recupera una o más métricas de series temporales a partir de los datos de Performance Insights. `GetResourceMetrics` requiere una métrica y un periodo de tiempo y devuelve una respuesta con una lista de puntos de datos.

Por ejemplo, se Consola de administración de AWS utiliza `GetResourceMetrics` para rellenar el gráfico de métricas del contador y el gráfico de carga de la base de datos, como se ve en la siguiente imagen.



Todas las métricas que devuelve `GetResourceMetrics` son métricas de series temporales estándar con la excepción de `db.load`. Esta métrica se muestra en el gráfico Database Load (Carga de base de datos). La métrica `db.load` es distinta de las demás métricas de series temporales porque puede desglosarla en subcomponentes llamados dimensiones. En la imagen anterior, `db.load` está desglosado y agrupado por los estados de espera que forman el `db.load`.

> **Note**
>
> `GetResourceMetrics` también puede devolver la métrica `db.sampleload`, pero la métrica `db.load` es apropiada en la mayoría de los casos.

Para obtener información sobre las métricas de contador devueltas por `GetResourceMetrics`, consulte Métricas de contador para Información sobre rendimiento.

Para las métricas se admiten los siguientes cálculos:

- Media: el valor medio de la métrica durante un período de tiempo. Añada `.avg` al nombre de la métrica.

- Mínimo: el valor mínimo de la métrica durante un período de tiempo. Añada `.min` al nombre de la métrica.
- Máximo: el valor máximo de la métrica durante un período de tiempo. Añada `.max` al nombre de la métrica.
- Suma: la suma de los valores de la métrica durante un periodo de tiempo. Añada `.sum` al nombre de la métrica.
- Número de muestras: El número de veces que se recopiló la métrica durante un período de tiempo. Añada `.sample_count` al nombre de la métrica.

Supongamos, por ejemplo, que una métrica se recopila durante 300 segundos (5 minutos) y que la métrica se recopila una vez cada minuto. Los valores para cada minuto son 1, 2, 3, 4 y 5. En este caso, se devuelven los siguientes cálculos:

- Media: 3
- Mínimo: 1
- Máximo: 5
- Suma: 15
- Número de muestras: 5

Para obtener información sobre el uso del `get-resource-metrics` AWS CLI comando, consulte `get-resource-metrics`.

Para la opción `--metric-queries`, especifique una o más consultas para las que desea obtener resultados. Cada consulta consta de un parámetro `Metric` obligatorio y de parámetros opcionales `GroupBy` y `Filter`. A continuación, se muestra un ejemplo de una especificación de opción `--metric-queries`.

```
{
   "Metric": "string",
   "GroupBy": {
     "Group": "string",
     "Dimensions": ["string", ...],
     "Limit": integer
   },
   "Filter": {"string": "string"
     ...}
```

AWS CLI ejemplos de Performance Insights

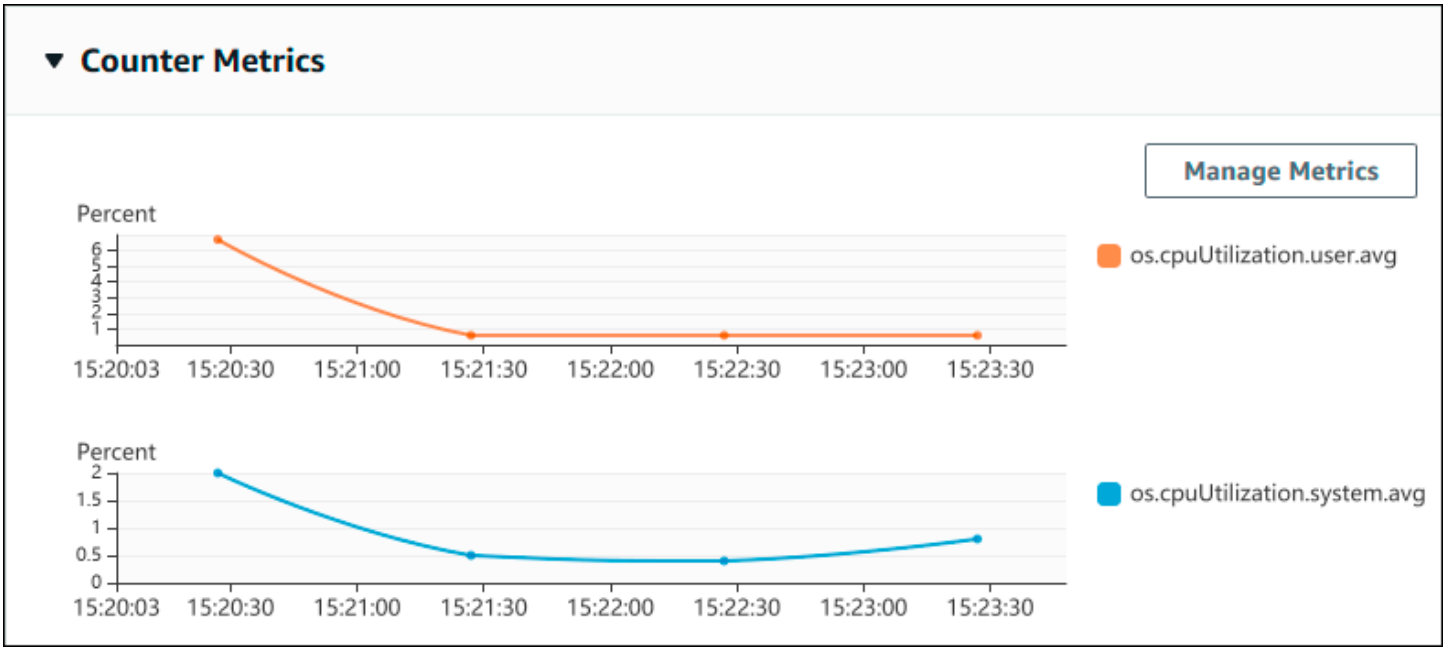
Los siguientes ejemplos muestran cómo utilizarla AWS CLI para Performance Insights.

Temas

- Recuperación de métricas de contador
- Recuperación del promedio de carga de base de datos para los eventos de espera principales
- Recuperación del promedio de carga de base de datos para las instrucciones de consulta principales
- Recuperación del promedio de carga de base de datos filtrado por consulta

Recuperación de métricas de contador

La siguiente captura de pantalla muestra dos gráficos de métricas de contador en la Consola de administración de AWS.



El siguiente ejemplo muestra cómo recopilar los mismos datos que utiliza la Consola de administración de AWS para generar los dos gráficos de métricas de contador.

Para Linux, macOS o Unix:

```
aws pi get-resource-metrics \
   --service-type DOCDB \
```

```
   --identifier db-ID \
   --start-time 2022-03-13T8:00:00Z \
   --end-time   2022-03-13T9:00:00Z \
   --period-in-seconds 60 \
   --metric-queries '[{"Metric": "os.cpuUtilization.user.avg"  },
                      {"Metric": "os.cpuUtilization.idle.avg"}]'
```

Para Windows:

```
aws pi get-resource-metrics ^
   --service-type DOCDB ^
   --identifier db-ID ^
   --start-time 2022-03-13T8:00:00Z ^
   --end-time   2022-03-13T9:00:00Z ^
   --period-in-seconds 60 ^
   --metric-queries '[{"Metric": "os.cpuUtilization.user.avg"  },
                      {"Metric": "os.cpuUtilization.idle.avg"}]'
```

También puede hacer que un comando sea más fácil de leer especificando un archivo para la opción `--metrics-query`. El siguiente ejemplo utiliza un archivo llamado query.json para la opción. El archivo tiene el siguiente contenido.

```
[
    {
        "Metric": "os.cpuUtilization.user.avg"
    },
    {
        "Metric": "os.cpuUtilization.idle.avg"
    }
]
```

Ejecute el siguiente comando para utilizar el archivo.

Para Linux, macOS o Unix:

```
aws pi get-resource-metrics \
   --service-type DOCDB \
   --identifier db-ID \
   --start-time 2022-03-13T8:00:00Z \
   --end-time   2022-03-13T9:00:00Z \
   --period-in-seconds 60 \
```

```
   --metric-queries file://query.json
```

Para Windows:

```
aws pi get-resource-metrics ^
   --service-type DOCDB ^
   --identifier db-ID ^
   --start-time 2022-03-13T8:00:00Z ^
   --end-time   2022-03-13T9:00:00Z ^
   --period-in-seconds 60 ^
   --metric-queries file://query.json
```

El ejemplo anterior especifica los siguientes valores para las opciones:

- `--service-type`: DOCDB para Amazon DocumentDB
- `--identifier`: el ID de recurso para la instancia de base de datos
- `--start-time` y:`--end-time` los valores ISO 8601 `DateTime` para el periodo de consulta, con varios formatos admitidos

Consulta durante un intervalo de una hora:

- `--period-in-seconds`: `60` para una consulta por minuto
- `--metric-queries`: una matriz de dos consultas, cada una para una métrica.

  El nombre de la métrica utiliza puntos para clasificar la métrica en categorías útiles y el elemento final es una función. En el ejemplo, la función es `avg` para cada consulta. Al igual que en Amazon CloudWatch, las funciones compatibles son `min`,`max`,`total`, `avg`.

La respuesta tiene un aspecto similar a la siguiente.

```
{
    "AlignedStartTime": "2022-03-13T08:00:00+00:00",
    "AlignedEndTime": "2022-03-13T09:00:00+00:00",
    "Identifier": "db-NQF3TTMFQ3GTOKIMJODMC3KQQ4",
    "MetricList": [
        {
            "Key": {
                "Metric": "os.cpuUtilization.user.avg"
            },
```

```
            "DataPoints": [
                {
                    "Timestamp": "2022-03-13T08:01:00+00:00", //Minute1
                    "Value": 3.6
                },
                {
                    "Timestamp": "2022-03-13T08:02:00+00:00", //Minute2
                    "Value": 2.6
                },
                //.... 60 datapoints for the os.cpuUtilization.user.avg metric
        {
            "Key": {
                "Metric": "os.cpuUtilization.idle.avg"
            },
            "DataPoints": [
                {
                    "Timestamp": "2022-03-13T08:01:00+00:00",
                    "Value": 92.7
                },
                {
                    "Timestamp": "2022-03-13T08:02:00+00:00",
                    "Value": 93.7
                },
                //.... 60 datapoints for the os.cpuUtilization.user.avg metric
            ]
        }
    ] //end of MetricList
} //end of response
```

La respuesta tiene `Identifier`, `AlignedStartTime` y `AlignedEndTime`. Como el valor `--period-in-seconds` era `60`, los tiempos de inicio y final se han alineado con el minuto. Si el `--period-in-seconds` fuera `3600`, los tiempos de inicio y final se habrían alineado con la hora.

La `MetricList` en la respuesta tiene una serie de entradas, cada una con una entrada `Key` y una entrada `DataPoints`. Cada `DataPoint` tiene un `Timestamp` y un `Value`. Cada lista de `Datapoints` tiene 60 puntos de datos porque las consultas son datos por minuto sobre una hora, con `Timestamp1/Minute1`, `Timestamp2/Minute2` y así sucesivamente, hasta `Timestamp60/Minute60`.

Como la consulta es para dos métricas de contador distintas, hay dos elementos en la respuesta `MetricList`.

Recuperación del promedio de carga de base de datos para los eventos de espera principales

El siguiente ejemplo es la misma consulta que se Consola de administración de AWS utiliza para generar un gráfico de líneas de área apilada. Este ejemplo recupera el `db.load.avg` durante la última hora con la carga dividida según los siete eventos de espera principales. El comando es el mismo que el comando en Recuperación de métricas de contador. Sin embargo, el archivo query.json tiene los elementos indicados a continuación.

```
[
    {
        "Metric": "db.load.avg",
        "GroupBy": { "Group": "db.wait_state", "Limit": 7 }
    }
]
```

Ejecute el comando siguiente.

Para Linux, macOS o Unix:

```
aws pi get-resource-metrics \
   --service-type DOCDB \
   --identifier db-ID \
   --start-time 2022-03-13T8:00:00Z \
   --end-time   2022-03-13T9:00:00Z \
   --period-in-seconds 60 \
   --metric-queries file://query.json
```

Para Windows:

```
aws pi get-resource-metrics ^
   --service-type DOCDB ^
   --identifier db-ID ^
   --start-time 2022-03-13T8:00:00Z ^
   --end-time   2022-03-13T9:00:00Z ^
   --period-in-seconds 60 ^
   --metric-queries file://query.json
```

El ejemplo especifica la métrica de `db.load.avg` y un `GroupBy` de los siete eventos de espera principales. Para obtener más información sobre los valores válidos para este ejemplo, consulte DimensionGroupla Referencia de la API Performance Insights.

La respuesta tiene un aspecto similar a la siguiente.

```
{
    "AlignedStartTime": "2022-04-04T06:00:00+00:00",
    "AlignedEndTime": "2022-04-04T06:15:00+00:00",
    "Identifier": "db-NQF3TTMFQ3GTOKIMJODMC3KQQ4",
    "MetricList": [
        {//A list of key/datapoints
            "Key": {
                //A Metric with no dimensions. This is the total db.load.avg
                "Metric": "db.load.avg"
            },
            "DataPoints": [
                //Each list of datapoints has the same timestamps and same number of
 items
                {
                    "Timestamp": "2022-04-04T06:01:00+00:00",//Minute1
                    "Value": 0.0
                },
                {
                    "Timestamp": "2022-04-04T06:02:00+00:00",//Minute2
                    "Value": 0.0
                },
                //... 60 datapoints for the total db.load.avg key
                ]
        },
        {
            "Key": {
                //Another key. This is db.load.avg broken down by CPU
                "Metric": "db.load.avg",
                "Dimensions": {
                    "db.wait_state.name": "CPU"
                }
            },
            "DataPoints": [
                {
                    "Timestamp": "2022-04-04T06:01:00+00:00",//Minute1
                    "Value": 0.0
                },
                {
                    "Timestamp": "2022-04-04T06:02:00+00:00",//Minute2
                    "Value": 0.0
                },
                //... 60 datapoints for the CPU key
```

```
            ]
        },//... In total we have 3 key/datapoints entries, 1) total, 2-3) Top Wait
 States
    ] //end of MetricList
} //end of response
```

En esta respuesta, hay tres entradas en la `MetricList`. Hay una entrada para el `db.load.avg` total y tres entradas para el `db.load.avg` divididas según uno de los siete eventos de espera principales. A diferencia del primer ejemplo, como había una dimensión de agrupación, debe haber una clave para cada agrupación de la métrica. No puede haber solo una clave para cada métrica, como en el caso de uso de métrica de contador básica.

Recuperación del promedio de carga de base de datos para las instrucciones de consulta principales

El siguiente ejemplo agrupa `db.wait_state` por las 10 instrucciones de consulta principales. Hay dos grupos distintos para instrucciones de consulta:

- `db.query`: la instrucción de consulta completa, como `{"find":"customers","filter":{"FirstName":"Jesse"},"sort":{"key":{"$numberInt":"1"}}}`
- `db.query_tokenized`: la instrucción de consulta tokenizada, como `{"find":"customers","filter":{"FirstName":"?"},"sort":{"key":{"$numberInt":"?"}},"limit":{"$numberInt":"?"}}`

Al analizar el desempeño de la base de datos, puede resultar útil tener en cuenta instrucciones de consulta que solo se diferencien en sus parámetros como un elemento de lógica. Así pues, puede utilizar `db.query_tokenized` al consultar. Sin embargo, sobre todo cuando está interesado en `explain()`, a veces es más útil examinar instrucciones de consulta completas con parámetros. Existe una relación principal-secundaria entre instrucciones de consulta tokenizadas y completas, con varias instrucciones de consulta completas (secundarias) agrupadas bajo la misma instrucción de consulta tokenizada (principal).

El comando en este ejemplo es similar al comando en Recuperación del promedio de carga de base de datos para los eventos de espera principales. Sin embargo, el archivo query.json tiene los elementos indicados a continuación.

```
[
    {
        "Metric": "db.load.avg",
```

```
        "GroupBy": { "Group": "db.query_tokenized", "Limit": 10 }
    }
]
```

El siguiente ejemplo utiliza `db.query_tokenized`.

Para Linux, macOS o Unix:

```
aws pi get-resource-metrics \
   --service-type DOCDB \
   --identifier db-ID \
   --start-time 2022-03-13T8:00:00Z \
   --end-time   2022-03-13T9:00:00Z \
   --period-in-seconds 3600 \
   --metric-queries file://query.json
```

Para Windows:

```
aws pi get-resource-metrics ^
   --service-type DOCDB ^
   --identifier db-ID ^
   --start-time 2022-03-13T8:00:00Z ^
   --end-time   2022-03-13T9:00:00Z  ^
   --period-in-seconds 3600 ^
   --metric-queries file://query.json
```

En este ejemplo, las consultas duran más de 1 hora y 1 minuto period-in-seconds.

El ejemplo especifica la métrica de `db.load.avg` y un `GroupBy` de los siete eventos de espera principales. Para obtener más información sobre los valores válidos para este ejemplo, consulte DimensionGroupla Referencia de la API Performance Insights.

La respuesta tiene un aspecto similar a la siguiente.

```
{
    "AlignedStartTime": "2022-04-04T06:00:00+00:00",
    "AlignedEndTime": "2022-04-04T06:15:00+00:00",
    "Identifier": "db-NQF3TTMFQ3GTOKIMJODMC3KQQ4",
    "MetricList": [
        {//A list of key/datapoints
            "Key": {
                "Metric": "db.load.avg"
```

```
            },
            "DataPoints": [
                //... 60 datapoints for the total db.load.avg key
                ]
        },
               {
            "Key": {//Next key are the top tokenized queries
                "Metric": "db.load.avg",
                "Dimensions": {
                    "db.query_tokenized.db_id": "pi-1064184600",
                    "db.query_tokenized.id": "77DE8364594EXAMPLE",
                    "db.query_tokenized.statement": "{\"find\":\"customers\",\"filter
\":{\"FirstName\":\"?\"},\"sort\":{\"key\":{\"$numberInt\":\"?\"}},\"limit\"
:{\"$numberInt\":\"?\"},\"$db\":\"myDB\",\"$readPreference\":{\"mode\":\"primary\"}}"
                }
            },
            "DataPoints": [
            //... 60 datapoints
            ]
        },
        // In total 11 entries, 10 Keys of top tokenized queries, 1 total key
    ] //End of MetricList
} //End of response
```

Esta respuesta tiene 11 entradas en la `MetricList` (1 total, 10 consultas tokenizadas principales) y cada entrada tiene 24 `DataPoints` por hora.

Para consultas tokenizadas, hay tres entradas en cada lista de dimensiones:

- `db.query_tokenized.statement`: la instrucción de consulta tokenizada.
- `db.query_tokenized.db_id` : el ID sintético que Información sobre rendimiento genera para usted. Este ejemplo devuelve el ID sintético de `pi-1064184600`.
- `db.query_tokenized.id`: el ID de la consulta dentro del panel Performance Insights.

  En el Consola de administración de AWS, este ID se denomina Support ID. Se denomina así porque el identificador son datos que AWS Support puede examinar para ayudarle a solucionar un problema con la base de datos. AWS se toma muy en serio la seguridad y la privacidad de sus datos, y casi todos los datos se almacenan cifrados junto con el suyo AWS KMS key. Por lo tanto, nadie en su interior AWS puede ver estos datos. En el ejemplo anterior, tanto `tokenized.statement` como `tokenized.db_id` se almacenan cifrados. Si tiene algún problema con su base de datos, AWS Support puede ayudarlo consultando el ID de soporte.

Al realizar consultas, puede ser conveniente especificar un `Group` en `GroupBy`. Sin embargo, para un control de más precisión sobre los datos que se devuelven, especifique la lista de dimensiones. Por ejemplo, si todo lo que se necesita es `db.query_tokenized.statement`, entonces se puede añadir un atributo `Dimensions` al archivo query.json.

```
[
    {
        "Metric": "db.load.avg",
        "GroupBy": {
            "Group": "db.query_tokenized",
            "Dimensions":["db.query_tokenized.statement"],
            "Limit": 10
        }
    }
]
```

Recuperación del promedio de carga de base de datos filtrado por consulta

La consulta de API correspondiente en este ejemplo es similar al comando en Recuperación del promedio de carga de base de datos para las instrucciones de consulta principales. Sin embargo, el archivo query.json tiene los elementos indicados a continuación.

```
[
 {
        "Metric": "db.load.avg",
        "GroupBy": { "Group": "db.wait_state", "Limit": 5  },
        "Filter": { "db.query_tokenized.id": "AKIAIOSFODNN7EXAMPLE" }
    }
]
```

En esta respuesta, todos los valores se filtran según la contribución de la consulta tokenizada EXAMPLE especificada en el AKIAIOSFODNN7 archivo query.json. Las claves también podrían seguir un orden distinto de una consulta sin un filtro, porque la consulta filtrada afectaba a los cinco eventos de espera principales.

CloudWatch Métricas de Amazon para Performance Insights

Performance Insights publica automáticamente las métricas en Amazon CloudWatch. Se pueden consultar los mismos datos desde Performance Insights, pero tener las métricas integradas CloudWatch facilita la adición de CloudWatch alarmas. También resulta fácil añadir las métricas a paneles de CloudWatch existentes.

Métrica	Description (Descripción)
DBLoad	El número de sesiones activas de Amazon DocumentDB. Normalmente, necesita los datos del número promedio de sesiones activas. En Performance Insights, estos datos se consultan como `db.load.avg` .
DBLoadCPU	El número de sesiones activas cuyo tipo de evento de espera es CPU. En Información sobre rendimiento, estos datos se consultan como `db.load.avg` , filtrados por el tipo de evento de espera `CPU`.
DBLoadSin CPU	El número de sesiones activas cuyo tipo de evento de espera no es CPU.

> **Note**
>
> Estas métricas se publican CloudWatch solo si hay carga en la instancia de base de datos.

Puede examinar estas métricas mediante la CloudWatch consola AWS CLI, la o la CloudWatch API.

Por ejemplo, puede obtener las estadísticas de la `DBLoad` métrica ejecutando el get-metric-statisticscomando.

```
aws cloudwatch get-metric-statistics \
    --region ap-south-1 \
    --namespace AWS/DocDB \
    --metric-name DBLoad  \
    --period 360 \
    --statistics Average \
    --start-time 2022-03-14T8:00:00Z \
    --end-time 2022-03-14T9:00:00Z \
    --dimensions Name=DBInstanceIdentifier,Value=documentdbinstance
```

Este ejemplo genera un resultado similar al siguiente.

```
{
    "Datapoints": [
        {
            "Timestamp": "2022-03-14T08:42:00Z",
            "Average": 1.0,
            "Unit": "None"
        },
        {
            "Timestamp": "2022-03-14T08:24:00Z",
            "Average": 2.0,
            "Unit": "None"
        },
        {
            "Timestamp": "2022-03-14T08:54:00Z",
            "Average": 6.0,
            "Unit": "None"
        },
        {
            "Timestamp": "2022-03-14T08:36:00Z",
            "Average": 5.7,
            "Unit": "None"
        },
        {
            "Timestamp": "2022-03-14T08:06:00Z",
            "Average": 4.0,
            "Unit": "None"
        },
        {
            "Timestamp": "2022-03-14T08:00:00Z",
            "Average": 5.2,
            "Unit": "None"
        }
    ],
    "Label": "DBLoad"
}
```


Puede utilizar la función matemática de `DB_PERF_INSIGHTS` métricas de la CloudWatch consola para consultar las métricas de los contadores de Amazon DocumentDB Performance Insights. La función `DB_PERF_INSIGHTS` también incluye la métrica `DBLoad` intervalos de menos de un minuto. Puede configurar CloudWatch alarmas en estas métricas. Para obtener más información sobre cómo

crear una alarma, consulte Crear una alarma en las métricas del contador de Performance Insights a partir de una AWS base de datos.

Para obtener más información CloudWatch, consulta ¿Qué es Amazon CloudWatch? en la Guía del CloudWatch usuario de Amazon.

Métricas de contador para Información sobre rendimiento

Las métricas de contador son métricas de rendimiento de sistemas operativos en el panel de control de Información sobre rendimiento. Para ayudar a identificar y analizar los problemas de rendimiento, puede correlacionar las métricas de contador con la carga de base de datos.

Contadores de sistemas operativos de Información de rendimiento

Los siguientes contadores de sistemas operativos están disponibles para Información sobre rendimiento para Amazon DocumentDB.

Contador	Tipo	Métrica
active (activa)	memory	os.memory.active
buffers	memory	os.memory.buffers
cached	memory	os.memory.cached
dirty	memory	os.memory.dirty
free	memory	os.memory.free
inactive	memory	os.memory.inactive
mapped	memory	os.memory.mapped
pageTables	memory	os.memory.pageTables
slab	memory	os.memory.slab
total	memory	os.memory.total
writeback	memory	os.memory.writeback

Contador	Tipo	Métrica
idle	cpuUtilization	os.cpuUtilization.idle
system	cpuUtilization	os.cpuUtilization.system
total	cpuUtilization	os.cpuUtilization.total
user	cpuUtilization	os.cpuUtilization.user
wait	cpuUtilization	os.cpuUtilization.wait
one	loadAverageMinute	Jos. loadAverageMinute.one
fifteen	loadAverageMinute	Jos. loadAverageMinute. quince
cinco	loadAverageMinute	así que. loadAverageMinute. cinco
cached	swap	os.swap.cached
free	swap	os.swap.free
in	swap	os.swap.in
out	swap	os.swap.out
total	swap	os.swap.total
rx	network	os.network.rx
tx	network	os.network.tx
num VCPUs	general	os.general.num VCPUs

Integración sin ETL con Amazon Service OpenSearch

Temas

- Amazon OpenSearch Service como destino
- Limitaciones

Amazon OpenSearch Service como destino

OpenSearch La integración de servicios con Amazon DocumentDB le permite transmitir eventos de carga completa y cambios de datos a OpenSearch los dominios. La infraestructura de ingestión se aloja como canalizaciones de OpenSearch ingestión y proporciona un mecanismo de alta escala y baja latencia para transmitir datos de forma continua desde las colecciones de Amazon DocumentDB.

Durante la carga completa, la integración sin ETL extrae primero los datos históricos a plena carga para utilizarlos en una canalización de ingestión. OpenSearch Una vez ingeridos los datos a plena carga, las canalizaciones de OpenSearch ingestión comenzarán a leer los datos de los flujos de cambios de Amazon DocumentDB y, finalmente, se pondrán al día para mantener la coherencia de los datos casi en tiempo real entre Amazon DocumentDB y. OpenSearch OpenSearch almacena los documentos en índices. Los datos entrantes de una colección de Amazon DocumentDB se pueden enviar a un índice o se pueden dividir en índices diferentes. Las canalizaciones de ingestión sincronizarán todos los eventos de creación, actualización y eliminación de una colección de Amazon DocumentDB según corresponda con la creación, actualización y eliminación OpenSearch de documentos para mantener ambos sistemas de datos sincronizados. Los canales de ingesta se pueden configurar para leer datos de una colección y escribirlos en un índice, o leer datos de una colección y enviarlos condicionalmente a varios índices.

Las canalizaciones de ingestión se pueden configurar para transmitir datos desde Amazon DocumentDB a OpenSearch Amazon Service mediante:

- Solo carga completa
- Transmisión de eventos de flujos de cambios desde Amazon DocumentDB sin carga completa
- Carga completa seguida de flujos de cambios desde Amazon DocumentDB

Para configurar la canalización de ingesta, siga estos pasos:

Paso 1: Crear un dominio de Amazon OpenSearch Service o una colección OpenSearch sin servidor

Se requiere una recopilación de Amazon OpenSearch Service con los permisos adecuados para leer los datos. Consulte Introducción a Amazon OpenSearch Service o Introducción a Amazon OpenSearch Serverless en la Guía para desarrolladores de Amazon OpenSearch Service para crear una colección. Consulte Amazon OpenSearch Ingestion en la Guía para desarrolladores de Amazon OpenSearch Service para crear un rol de AIM con los permisos correctos para acceder a los datos de escritura en la colección o el dominio.

Paso 2: habilitación de los flujos de cambios en el clúster de Amazon DocumentDB

Asegúrese de que los flujos de cambios estén habilitados en las colecciones requeridas del clúster de Amazon DocumentDB. Para obtener más información, consulte Uso de flujos de cambios con Amazon DocumentDB.

Paso 3: configuración del rol de canalización con permisos para escribir en el bucket de Amazon S3 y en el dominio o colección de destino

Una vez creada la colección de Amazon DocumentDB y habilitado el flujo de cambios, configure el rol de canalización que desee usar en la configuración de canalización y agregue los siguientes permisos al rol:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "allowReadAndWriteToS3ForExport",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:AbortMultipartUpload",
                "s3:PutObject",
                "s3:PutObjectAcl"
            ],
            "Resource": [
```

```
                "arn:aws:s3:::my-bucket/export/*"
            ]
        }
    ]
}
```

Para que una OpenSearch canalización escriba datos en un OpenSearch dominio, el dominio debe tener una política de acceso a nivel de dominio que permita al rol de canalización sts_role_arn acceder a ellos. El siguiente ejemplo de política de acceso al dominio permite que el rol de canalización denominado `pipeline-role`, que creó en el paso anterior, escriba datos en el dominio denominado `ingestion-domain`:

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::{your-account-id}:role/{pipeline-role}"
      },
      "Action": ["es:DescribeDomain", "es:ESHttp*"],
      "Resource": "arn:aws:es:{region}:{your-account-id}:domain/{domain-name}/*"
    }
  ]
}
```

Paso 4: agregación de los permisos necesarios en el rol de canalización para crear X-ENI

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachNetworkInterface",
                "ec2:CreateNetworkInterface",
                "ec2:CreateNetworkInterfacePermission",
```

```
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteNetworkInterfacePermission",
                "ec2:DetachNetworkInterface",
                "ec2:DescribeNetworkInterfaces"
            ],
            "Resource": [
                "arn:aws:ec2:*:420497401461:network-interface/*",
                "arn:aws:ec2:*:420497401461:subnet/*",
                "arn:aws:ec2:*:420497401461:security-group/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:Describe*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [ "ec2:CreateTags" ],
            "Resource": "arn:aws:ec2:*:*:network-interface/*",
            "Condition": {
               "StringEquals": { "aws:RequestTag/OSISManaged": "true" }
            }
        }
    ]
}
```

Paso 5: creación de la canalización

Configure una canalización OpenSearch de ingestión especificando Amazon DocumentDB como origen. En este ejemplo de configuración de canalización se presupone el uso de un mecanismo de obtención del flujo de cambios. Consulte Uso de una canalización OpenSearch de ingestión con Amazon DocumentDB en la Guía para desarrolladores de OpenSearch Amazon Service para obtener más información.

Limitaciones

Se aplican las siguientes limitaciones a la integración de Amazon DocumentDB: OpenSearch

- Solo se admite una colección de Amazon DocumentDB como origen por canalización.
- No se admite la ingesta de datos entre regiones. El clúster y el OpenSearch dominio de Amazon DocumentDB deben estar en la misma AWS región.
- No se admite la ingesta de datos entre cuentas. El clúster de Amazon DocumentDB y la canalización OpenSearch de ingestión deben estar en la misma cuenta. AWS
- No se admiten los clústeres elásticos de Amazon DocumentDB. Solo se admiten los clústeres basados en instancias de Amazon DocumentDB.
- Asegúrese de que el clúster de Amazon DocumentDB tenga habilitada la autenticación mediante AWS secretos. AWS los secretos son el único mecanismo de autenticación compatible.
- La configuración de canalización existente no se puede actualizar para ingerir datos de una base de datos diferente o de and/or una colección diferente. Para actualizar el nombre de la and/or colección de bases de datos de una canalización, debe crear una canalización nueva.

Uso de Amazon DocumentDB sin servidor

Amazon DocumentDB sin servidor es una configuración de escalado automático bajo demanda que automatiza los procesos de ajuste dinámico de la capacidad de la base de datos de Amazon DocumentDB en función de la demanda de las aplicaciones. Solo se le cobrará por los recursos que consuman los clústeres. Por lo tanto, DocumentDB sin servidor le permite mantenerse dentro del presupuesto y evitar pagar los recursos de computación que no utiliza.

Este tipo de automatización es especialmente valioso para entornos con cargas de trabajo muy variables e impredecibles, como bases de datos de multitenencia, bases de datos distribuidas y sistemas de desarrollo y pruebas.

Temas

- Casos de uso de DocumentDB sin servidor
- Ventajas de Amazon DocumentDB sin servidor
- Cómo funciona Amazon DocumentDB sin servidor
- Requisitos y limitaciones de DocumentDB sin servidor
- Creación de un clúster que utilice Amazon DocumentDB sin servidor
- Migración a Amazon DocumentDB sin servidor
- Administración de Amazon DocumentDB sin servidor
- Límites de instancias de Amazon DocumentDB sin servidor
- Configuración de escalado de Amazon DocumentDB sin servidor
- Supervisión de Amazon DocumentDB sin servidor

Casos de uso de DocumentDB sin servidor

Los clústeres aprovisionados de Amazon DocumentDB y DocumentDB sin servidor admiten muchos tipos de cargas de trabajo de base de datos, desde entornos de desarrollo y pruebas hasta las aplicaciones más exigentes y esenciales para la empresa que requieren una gran escala y disponibilidad. Sin embargo, DocumentDB sin servidor añade otra dimensión a las cargas de trabajo del cliente, a saber, la capacidad de admitir sitios web y aplicaciones que tienen cargas de trabajo impredecibles.

DocumentDB sin servidor es especialmente útil para los siguientes casos de uso:

- Cargas de trabajo variables: ejecuta cargas de trabajo que tienen un aumento de actividad repentino e impredecible. Un ejemplo de ello sería un sitio dedicado al tráfico, que experimenta un aumento repentino de la actividad cuando comienza a llover. Otro caso sería un sitio de comercio electrónico en el que aumenta el tráfico cuando se ofrecen ventas o promociones especiales. Con DocumentDB sin servidor, la capacidad de la base de datos se escala automáticamente para satisfacer las necesidades de los picos de carga de la aplicación y vuelve a disminuir cuando termina el aumento de actividad. Con DocumentDB sin servidor, ya no tiene que aprovisionar la capacidad para los picos ni para la carga promedio. Puede especificar un límite de capacidad superior para gestionar la peor situación. Esa capacidad no se utilizaría a menos que fuera necesario.
  - La granularidad de la reducción horizontal de DocumentDB sin servidor le permite adaptar la capacidad a las necesidades de su base de datos. En el caso de un clúster aprovisionado, el escalado vertical requiere añadir una nueva instancia. DocumentDB sin servidor puede agregar media DCU cuando solo se necesite un poco más de capacidad. Puede añadir 0,5, 1, 1,5, 2 o la mitad adicional en DCUs función de la capacidad adicional necesaria para gestionar un aumento de la carga de trabajo. Además, puede eliminar 0,5, 1, 1,5, 2 unidades o la mitad adicional DCUs cuando la carga de trabajo disminuye y esa capacidad ya no es necesaria.
- Aplicaciones de tenencias múltiples: con DocumentDB sin servidor, no precisa administrar individualmente la capacidad de la base de datos para cada aplicación de la flota. DocumentDB sin servidor administra la capacidad de las bases de datos individuales por usted.
  - Puede crear un clúster para cada inquilino. De esta forma, puede utilizar características como la clonación y la restauración de instantáneas para mejorar la alta disponibilidad y la recuperación ante desastres según corresponda para cada inquilino.
  - Cada inquilino puede tener períodos específicos de actividad e inactividad según la hora del día, la época del año, los eventos promocionales, etc. Cada clúster puede tener un amplio rango de capacidad. De esta forma, los clústeres con poca actividad incurren en los cargos mínimos de instancias. Cualquier clúster puede escalarse de forma vertical rápidamente para gestionar períodos de actividad elevada.
- Aplicaciones nuevas: si implementa una nueva aplicación y no está seguro del tamaño de instancia que necesita. Con DocumentDB sin servidor, puede configurar un clúster con una o varias instancias y hacer que la base de datos se escale automáticamente de acuerdo con los requisitos de capacidad de la aplicación.
- Aplicaciones de uso mixto: supongamos que tiene una aplicación de procesamiento de transacciones en línea (OLTP), pero periódicamente experimenta picos en el tráfico de consultas. Si especifica niveles de promoción para las instancias de DocumentDB sin servidor en un

clúster, puede configurar el clúster para que las instancias de lectura se puedan escalar independientemente de la instancia de escritura para gestionar la carga adicional. Cuando el pico de uso disminuye, las instancias de lectura se reducen verticalmente de nuevo para adaptarlas a la capacidad de la instancia de escritura.

- Planificación de capacidad: supongamos que normalmente ajusta la capacidad de la base de datos o verifica la capacidad de la base de datos óptima para la carga de trabajo modificando las clases de instancias de todas las instancias de un clúster. Con DocumentDB sin servidor, puede evitar esta sobrecarga administrativa. Para determinar la capacidad mínima y máxima apropiadas, puede ejecutar la carga de trabajo y comprobar cuánto se escalan realmente las instancias.
  - Puede modificar las instancias existentes de aprovisionadas a DocumentDB sin servidor o de DocumentDB sin servidor a aprovisionadas. En estos casos, no es necesario crear un clúster nuevo ni una instancia nueva.
- Desarrollo y pruebas: además de ejecutar las aplicaciones más exigentes, también puede utilizar DocumentDB sin servidor en entornos de desarrollo y pruebas. Con DocumentDB sin servidor, puede crear instancias con una capacidad mínima en lugar de utilizar clases de instancias ampliables db.t*. Puede establecer la capacidad máxima lo suficientemente alta como para que esas instancias puedan seguir ejecutando cargas de trabajo sustanciales sin quedarse sin memoria. Cuando la base de datos no está en uso, todas las instancias se reducen verticalmente para evitar cargos innecesarios.

Uso de Amazon DocumentDB sin servidor para las cargas de trabajo aprovisionadas existentes

Supongamos que ya tiene una aplicación de DocumentDB en ejecución en un clúster aprovisionado. Para comprobar cómo funcionaría la aplicación con DocumentDB sin servidor, añada una o varias instancias de DocumentDB sin servidor al clúster existente como instancias de lectura. Puede comprobar con qué frecuencia se escalan y reducen verticalmente las instancias de lectura. Puede utilizar el mecanismo de conmutación por error de DocumentDB para convertir una instancia sin servidor de DocumentDB en la redacción y comprobar cómo gestiona la carga de trabajo. read/write De esta forma, puede realizar el cambio con un tiempo de inactividad mínimo y sin cambiar el punto de conexión que utilizan las aplicaciones cliente. Para obtener más información sobre el procedimiento para convertir los clústeres existentes a DocumentDB sin servidor, consulte Migración a Amazon DocumentDB sin servidor.

Ventajas de Amazon DocumentDB sin servidor

DocumentDB sin servidor está destinado a cargas de trabajo variables o «con picos». Con cargas de trabajo tan impredecibles, podría tener dificultades para planificar cuándo cambiar la capacidad de la base de datos. También podría tener problemas para realizar cambios de capacidad con la suficiente rapidez mediante los mecanismos conocidos, como añadir instancias o cambiar clases de instancias. DocumentDB sin servidor ofrece las siguientes ventajas para facilitar estos casos de uso:

- Administración de la capacidad más sencilla que con la aprovisionada: DocumentDB sin servidor reduce el esfuerzo de planificar los tamaños de las instancias y cambiar el tamaño de las instancias a medida que cambia la carga de trabajo. También reduce el esfuerzo para mantener una capacidad uniforme para todas las instancias en un clúster.

- Escalado más rápido y sencillo durante períodos de alta actividad: DocumentDB sin servidor escala la capacidad de memoria y de computación en función de las necesidades, sin interrumpir las transacciones del cliente ni de la carga de trabajo general. La capacidad de utilizar instancias de lectura con DocumentDB sin servidor le permite aprovechar el escalado horizontal además del escalado vertical.

- Rentable durante los períodos de baja actividad: DocumentDB sin servidor ayuda a evitar el sobreaprovisionamiento de las instancias. DocumentDB sin servidor agrega recursos en incrementos granulares cuando las instancias se escalan verticalmente. Solo pagará por los recursos de la base de datos que consuma. El uso de recursos de DocumentDB sin servidor se mide por segundos. De esta forma, cuando una instancia se reduce verticalmente, la reducción del uso de recursos se registra de inmediato.

- Paridad de características con elementos aprovisionados: puede utilizar todas las funciones de DocumentDB con DocumentDB sin servidor. Por ejemplo, con DocumentDB serverless puede usar instancias de lectura, autenticación de bases de datos AWS Identity and Access Management (IAM) y Performance Insights.

  En particular, con DocumentDB sin servidor puede aprovechar las siguientes características de los clústeres aprovisionados:

  - Instancias de lectura: DocumentDB sin servidor puede aprovechar las instancias de lectura para escalar horizontalmente. Cuando un clúster contiene una o más instancias de lectura, el clúster

puede conmutar por error inmediatamente en caso de que haya problemas con la instancia de escritura.

- Clústeres Multi-AZ: puede distribuir las instancias sin servidor de DocumentDB de un clúster en varias zonas de disponibilidad (). AZs La configuración de un clúster Multi-AZ ayuda a garantizar la continuidad del negocio incluso en los raros casos en los que hay problemas que afectan a una AZ completa.

Cómo funciona Amazon DocumentDB sin servidor

Temas

- Descripción general de
- Configuraciones para clústeres de Amazon DocumentDB
- Capacidad de escalado de Amazon DocumentDB sin servidor
- Escalado de Amazon DocumentDB sin servidor
- Estado inactivo (0,5) DCUs

Descripción general de

Amazon DocumentDB sin servidor es adecuado para la mayoría de las cargas de trabajo más exigentes y muy variables. Por ejemplo, el uso de la base de datos puede ser intensivo durante un corto periodo de tiempo, seguido de largos periodos de poca actividad o de ninguna actividad en absoluto. Ejemplos de ello son sitios web de venta minorista, juegos o deportes con eventos promocionales periódicos y bases de datos que generan informes cuando se necesitan. Otros son entornos de desarrollo y pruebas y nuevas aplicaciones en las que el uso podría aumentar rápidamente. Para casos como estos y muchos otros, la configuración correcta de la capacidad por anticipado no siempre es posible con el modelo aprovisionado. También puede resultar en costos más elevados si se aprovisiona en exceso y tiene capacidad que no utiliza.

En cambio, los clústeres aprovisionados de DocumentDB son adecuados para cargas de trabajo estables. Con los clústeres aprovisionados, puede elegir una clase de instancia que tenga una cantidad predefinida de memoria, potencia de CPU, I/O ancho de banda, etc. Si la carga de trabajo cambia, modificará manualmente la clase del escritor y los lectores. El modelo aprovisionado funciona bien cuando se puede ajustar con anticipación la capacidad de los patrones de consumo esperados y se aceptan interrupciones breves mientras cambia la clase del escritor y los lectores del clúster.

DocumentDB sin servidor está diseñado desde cero para admitir clústeres sin servidor que son escalables instantáneamente. DocumentDB sin servidor está diseñado para proporcionar el mismo grado de seguridad y aislamiento que los lectores y escritores aprovisionados. Estos aspectos son cruciales en entornos de nube sin servidor multitenant. El mecanismo de escalado dinámico tiene muy poca sobrecarga para que pueda responder rápidamente a los cambios en la carga de trabajo de la base de datos. También es lo suficientemente potente como para satisfacer los incrementos drásticos en la demanda de procesamiento.

Con DocumentDB sin servidor, podrá crear un clúster de DocumentDB sin quedar sujeto a una capacidad de base de datos específica para cada escritor y lector. El usuario especifica el rango mínimo y máximo de capacidad. DocumentDB escala cada escritor o lector de DocumentDB sin servidor en el clúster dentro de ese rango de capacidad. Usar un clúster Multi-AZ en el que cada escritor o lector puede escalar dinámicamente permite aprovechar el escalado dinámico y de una alta disponibilidad.

DocumentDB sin servidor escala los recursos de base de datos de forma automática en función de las especificaciones de capacidad mínima y máxima. El escalado es rápido, ya que la mayoría de las operaciones de eventos de escalado mantienen al escritor o al lector en el mismo host. En los raros casos en que un escritor o lector de DocumentDB sin servidor se mueve de un host a otro, DocumentDB sin servidor administra las conexiones automáticamente. No es necesario cambiar el código de la aplicación cliente de base de datos o las cadenas de conexión de base de datos.

Con DocumentDB sin servidor, al igual que ocurre con los clústeres aprovisionados, la capacidad de almacenamiento y la capacidad informática son independientes. Cuando hablamos de capacidad y escalado de DocumentDB sin servidor, nos referimos siempre a la capacidad informática que aumenta o disminuye. Por lo tanto, el clúster puede contener muchos terabytes de datos incluso cuando la capacidad de la CPU y la memoria se reducen a niveles bajos.

En lugar de aprovisionar y administrar los servidores de bases de datos, hay que especificar la capacidad de la base de datos. La capacidad real de cada instancia de escritura o lectura de DocumentDB sin servidor varía con el tiempo, según la carga de trabajo. Para obtener más información sobre este mecanismo, consulte Escalado de Amazon DocumentDB sin servidor.

Configuraciones para clústeres de Amazon DocumentDB

Para cada uno de sus clústeres de Amazon DocumentDB, puede elegir cualquier combinación de capacidad de DocumentDB sin servidor, capacidad aprovisionada o ambas.

Puede configurar un clúster que contenga tanto capacidad aprovisionada como capacidad de DocumentDB sin servidor. A esto se lo conoce como clúster de configuración mixta. Por ejemplo, supongamos que necesita más read/write capacidad de la disponible para un escritor sin servidor de DocumentDB. En este caso, puede configurar el clúster con un escritor aprovisionado muy grande. Entonces, aún puede usar DocumentDB sin servidor para los lectores. O, supongamos que la carga de trabajo de escritura del clúster varía pero la carga de trabajo de lectura es estable. En este caso, puede configurar el clúster con un escritor de DocumentDB sin servidor y uno o más lectores aprovisionados.

También puede configurar un clúster en el que DocumentDB sin servidor administre toda la capacidad. Para ello, puede crear un nuevo clúster y utilizar DocumentDB sin servidor desde el principio. O bien, puede reemplazar toda la capacidad aprovisionada de un clúster existente con DocumentDB sin servidor. Para conocer los procedimientos para crear un nuevo clúster con DocumentDB sin servidor o para cambiar un clúster existente a DocumentDB sin servidor, consulte Creación de un clúster que utilice Amazon DocumentDB sin servidor y Migración a Amazon DocumentDB sin servidor.

Si no utiliza DocumentDB sin servidor en absoluto en un clúster, todos los escritores y lectores del clúster serán aprovisionados. Este es el tipo de clúster más común con el que la mayoría de los usuarios están familiarizados. La capacidad aprovisionada es constante. Los cargos son relativamente fáciles de pronosticar. No obstante, debe predecir de antemano cuánta capacidad necesita. En algunos casos, las predicciones pueden ser inexactas o las necesidades de capacidad pueden cambiar. En estos casos, el clúster puede estar infraprovisionado (más lento de lo que se desea) o sobreaprovisionado (más caro de lo que se desea).

Capacidad de escalado de Amazon DocumentDB sin servidor

La unidad de medida de Amazon DocumentDB sin servidor es la unidad de capacidad de DocumentDB (DCU). La capacidad de escalado de DocumentDB sin servidor no está vinculada a las clases de instancias que utiliza para los clústeres aprovisionados.

Cada DCU es una combinación de aproximadamente 2 gigabytes (GiB) de memoria, la CPU correspondiente y las redes. El rango de capacidad de la base de datos se especifica mediante esta unidad de medida. Las métricas `ServerlessDatabaseCapacity` y `DCUUtilization` CloudWatch le ayudan a determinar cuánta capacidad está utilizando realmente su base de datos y dónde se encuentra dentro del rango especificado.

Cada escritor o lector de DocumentDB sin servidor tiene una capacidad en un momento dado. La capacidad es un número de punto flotante que representa. DCUs La capacidad aumenta o disminuye

cada vez que el escritor o el lector se escalan. Este valor se mide cada segundo. Para cada clúster en el que se pretende utilizar DocumentDB sin servidor, se define un rango de capacidad: los valores de capacidad mínima y máxima entre los que puede escalar cada escritor o lector de DocumentDB sin servidor. El rango de capacidad es el mismo para cada escritor o lector de DocumentDB sin servidor en un clúster. Cada escritor o lector de DocumentDB sin servidor tiene su propia capacidad, la cual corresponderá a algún punto en ese rango.

DocumentDB serverless es compatible con DocumentDB 5.0.0 y versiones posteriores con un rango de capacidad de 0,5 a 256. DCUs

La capacidad sin servidor de DocumentDB más pequeña que puede definir es 0,5. DCUs Puede especificar un número mayor si es menor o igual que el valor de capacidad máxima admitida. Si se establece la capacidad mínima en un número pequeño, los clústeres cargados ligeramente consumen recursos informáticos mínimos. Al mismo tiempo, permanecen listos para aceptar conexiones de inmediato y ampliarse cuando están ocupados.

Recomendamos establecer el mínimo en un valor que permita a cada instancia de escritura o lectura mantener el conjunto de trabajo de la aplicación en el grupo del búfer. De esta forma, el contenido del grupo del búfer no se desecha durante los períodos de inactividad. Para saber todo lo que debe tener en cuenta a la hora de elegir el rango de capacidad de escalado, consulte Selección del rango de capacidad de escalado para un clúster de DocumentDB sin servidor.

En función de cómo configure los lectores en una implementación multi-AZ, sus capacidades se pueden vincular a la capacidad del escritor o de forma independiente. Para obtener información detallada sobre cómo hacerlo, consulte Visualización y modificación del nivel de promoción de los lectores sin servidor.

Supervisar DocumentDB sin servidor implica medir los valores de capacidad del escritor y los lectores del clúster a lo largo del tiempo. Si la base de datos no se reduce a la capacidad mínima, puede realizar acciones como ajustar el mínimo y optimizar la aplicación de base de datos. Si la base de datos alcanza su capacidad máxima de forma coherente, puede realizar acciones como aumentar el máximo. También puede optimizar la aplicación de base de datos y distribuir la carga de consultas entre más lectores.

Los cargos correspondientes a la capacidad de DocumentDB sin servidor se miden en términos de horas de DCU. Para obtener información sobre cómo se calculan los cargos de DocumentDB sin servidor, consulte los Precios de Amazon DocumentDB. Supongamos que el número total de escritores y lectores del clúster es n. En ese caso, el clúster consume aproximadamente n x como mínimo DCUs cuando no se ejecuta ninguna operación de base de datos. Amazon DocumentDB

podría ejecutar operaciones de supervisión o mantenimiento que provocan una pequeña cantidad de carga. Ese clúster no consume más de n x como máximo DCUs cuando la base de datos se ejecuta a plena capacidad.

Para obtener más información sobre cómo elegir los valores de DCU mínimos y máximos adecuados, consulte Selección del rango de capacidad de escalado para un clúster de DocumentDB sin servidor. Los valores mínimo y máximo de DCU que especifica también afectan a algunos límites de instancias de Amazon DocumentDB. Para obtener información detallada sobre la interacción entre el rango de capacidad y los límites de la instancia, consulte Límites de instancias de Amazon DocumentDB sin servidor.

Escalado de Amazon DocumentDB sin servidor

Para cada escritor o lector de DocumentDB sin servidor, Amazon DocumentDB realiza un seguimiento continuo del uso de recursos como la CPU, la memoria y la red. Estas mediciones se denominan colectivamente carga. La carga incluye las operaciones de base de datos realizadas por la aplicación. También incluye procesamiento en segundo plano para el servidor de base de datos y tareas administrativas de Amazon DocumentDB. Cuando la capacidad se ve limitada por alguno de estos factores, DocumentDB sin servidor se escala verticalmente. DocumentDB sin servidor también se escala verticalmente cuando detecta problemas de rendimiento que se pueden resolver de esta manera. Puede supervisar la utilización de los recursos y cómo afecta el escalado en DocumentDB sin servidor mediante los procedimientos en Supervisión de Amazon DocumentDB sin servidor.

La carga puede variar según el escritor o los lectores del clúster. El escritor controla las operaciones de escritura y realiza todas las modificaciones de los datos en el volumen del clúster. Los lectores pueden procesar solicitudes de solo lectura.

El escalado es la operación que aumenta o disminuye la capacidad de DocumentDB sin servidor para la base de datos. Con DocumentDB serverless, cada escritor y lector tiene su propio valor de capacidad actual, medido en. DCUs DocumentDB sin servidor escala un escritor o lector hasta una capacidad superior cuando su capacidad actual es demasiado baja para gestionar la carga. Escala el escritor o el lector a una capacidad inferior cuando su capacidad en uso es superior a la necesaria.

DocumentDB sin servidor puede aumentar la capacidad de forma incremental. Cuando la demanda de carga de trabajo comienza a alcanzar la capacidad de base de datos actual de un escritor o lector, DocumentDB serverless aumenta la cantidad de DCUs ese escritor o lector. DocumentDB sin servidor escala la capacidad en función de los incrementos necesarios para proporcionar el mejor rendimiento de los recursos consumidos. El escalado se produce en incrementos tan pequeños

como 0,5. DCUs Cuanto mayor sea la capacidad en uso, mayor será el incremento de escalado y, por lo tanto, más rápido puede producirse el escalado.

Ya que el escalado en DocumentDB sin servidor es tan frecuente, granular y no disruptivo, no genera eventos discretos en la Consola de administración de AWS. En su lugar, puedes medir las CloudWatch métricas de Amazon, como `serverlessDatabaseCapacity` y`DCUUtilization`, y realizar un seguimiento de sus valores mínimo, máximo y promedio a lo largo del tiempo. Para obtener más información sobre la supervisión de DocumentDB sin servidor, consulte Supervisión de Amazon DocumentDB sin servidor.

El escalado vertical o la reducción vertical pueden deberse a lo siguiente:

- Utilización de memoria
- Utilización de la CPU
- Utilización de la red
- Uso del almacenamiento

Puede supervisar estas causas del escalado up/down en las instancias sin servidor de DocumentDB. Para obtener más información, consulte Supervisión de Amazon DocumentDB sin servidor.

Puede elegir escalar el lector al mismo tiempo que el escritor asociado o independientemente del escritor. Para ello, especifique el nivel de promoción de ese lector.

- Los lectores de DocumentDB sin servidor, en niveles de promoción 0 y 1, se escalan al mismo tiempo que el escritor. Este comportamiento de escalado hace que los lectores de los niveles prioritarios 0 y 1 sean ideales para disponibilidad. Esto se debe a que siempre tienen el tamaño adecuado para asumir la carga de trabajo de escritura en caso de conmutación por error.
- Los lectores de los niveles de promoción 2 a 15 escalan independientemente del escritor. Cada lector se mantiene dentro de los valores de DCU mínimo y máximo especificados para el clúster. Cuando un lector escala independientemente de la base de datos de escritura asociada, puede pasar a quedar inactiva y reducirse mientras el escritor continúa procesando un gran volumen de transacciones. Sigue disponible como objetivo de conmutación por error si no hay otros lectores disponibles en niveles de promoción más bajos. No obstante, si se promueve para ser el escritor, es posible que tenga que escalar para manejar toda la carga de trabajo del escritor.

Para obtener más información sobre cómo ver y cambiar los niveles de promoción de las instancias sin servidor, consulte Visualización y modificación del nivel de promoción de los lectores sin servidor.

El escalado de DocumentDB sin servidor puede ocurrir mientras las conexiones de la base de datos están abiertas, mientras las transacciones están en proceso, etc. DocumentDB sin servidor no espera a que llegue un punto de inactividad para empezar el escalado. El escalado no interrumpe ninguna operación de base de datos en curso.

Si la carga de trabajo requiere más capacidad de lectura de la disponible con un solo escritor y un solo lector, puede agregar lectores múltiples de DocumentDB sin servidor al clúster. Cada lector de DocumentDB sin servidor puede escalar dentro de los valores de capacidad mínimo y máximo especificados para su clúster. Puede utilizar el punto de conexión del lector del clúster para dirigir las sesiones de solo lectura a los lectores y reducir la carga en el escritor.

Que DocumentDB sin servidor realice un escalado y la rapidez con la que se producirá el escalado una vez que se inicie también dependerán de la configuración de DCU mínima y máxima para el clúster. Además, depende de si un lector está configurado para escalar junto con el escritor o independientemente de él. Para obtener información detallada sobre la configuración del escalado, consulte Configuración de escalado de Amazon DocumentDB sin servidor.

Estado inactivo (0,5) DCUs

Cuando los lectores o lectores sin servidor de Amazon DocumentDB están inactivos, las instancias sin servidor de DocumentDB admiten la reducción a un estado inactivo de 0,5 DCUs si el clúster está MinCapacity configurado en 0,5.

En estado inactivo, las instancias de DocumentDB sin servidor no tienen suficiente capacidad de procesamiento de CPU para admitir la mayoría de las cargas de trabajo de producción, pero están listas para escalarse verticalmente con rapidez para admitir una nueva carga de trabajo. En un estado no inactivo, las instancias sin servidor de DocumentDB suelen requerir al menos entre 1,0 y 2,5. DCUs Por lo tanto, cuando las instancias sin servidor de DocumentDB escalen de un estado inactivo a un estado no inactivo, se escalarán directamente de 1,0 a 2,5 DCUs (o el valor de MaxCapacity si es inferior).

Para permitir la reducción a 0,5 DCUs cuando están inactivas, los límites de instancias se limitan si se configura para que sea inferior o igual a 1,0. MinCapacity DCUs Para obtener más información sobre cómo afecta la MinCapacity configuración a los límites, consulteLímites de instancias de Amazon DocumentDB sin servidor.

Requisitos y limitaciones de DocumentDB sin servidor

Requisitos de características

Disponibilidad por región

El tipo de instancia de Amazon DocumentDB sin servidor está disponible en las siguientes regiones:

El siguiente AWS CLI comando se puede usar para verificar las opciones exactas de instancia sin servidor de DocumentDB que se ofrecen en una región determinada:

```
aws docdb describe-orderable-db-instance-options \
        --region my_region \
        --db-instance-class db.serverless \
        --engine docdb
```

Disponibilidad de la versión del motor

DocumentDB sin servidor es compatible con la versión del motor Amazon DocumentDB 5.0.0.

> **Note**
>
> DocumentDB sin servidor es compatible solamente con las versiones de parche 5.0.0 más recientes. Asegúrese de que su clúster esté actualizado a una versión reciente del parche del motor. Para obtener más información sobre el mantenimiento de los clústeres de Amazon DocumentDB, consulte Mantenimiento de Amazon DocumentDB.

Configuración del clúster

Antes de añadir cualquier instancia de Amazon DocumentDB sin servidor a un clúster de Amazon DocumentDB, el clúster también debe tener el conjunto de parámetros `ServerlessV2ScalingConfiguration`. Esto define el rango de capacidad de las instancias de DocumentDB sin servidor en el clúster. Para obtener más información sobre la configuración de escalado, consulte Configuración de escalado de Amazon DocumentDB sin servidor.

Configuración del rango mínimo de capacidad de escalado para determinadas características de Amazon DocumentDB

Algunas características de Amazon DocumentDB funcionan con DocumentDB sin servidor, pero esto podría causar problemas si el rango de capacidad es inferior al necesario para los requisitos de memoria de esas características con su carga de trabajo específica. En ese caso, es posible que la base de datos no funcione tan bien como de costumbre o que presente errores. out-of-memory

Las siguientes funciones requieren una configuración de un `MinCapacity` and/or `MaxCapacity` valor superior para un funcionamiento óptimo:

- Información de rendimiento
- Creación de instancias sin servidor en un clúster con un gran volumen de datos

  Esto incluye la creación de instancias sin servidor como parte de la restauración de un clúster.

Para obtener recomendaciones sobre cómo configurar el rango de capacidad adecuado (si está utilizando esta característica), consulte Selección del rango de capacidad de escalado para un clúster de DocumentDB sin servidor. Para obtener información sobre la solución de problemas si la base de datos encuentra out-of-memory errores debido a un rango de capacidad mal configurado, consulteEvitar errores out-of-memory.

Limitaciones de características

Las siguientes características de las instancias aprovisionadas de Amazon DocumentDB no están disponibles para las instancias de DocumentDB sin servidor:

- Clústeres globales

Creación de un clúster que utilice Amazon DocumentDB sin servidor

Creación de un clúster de Amazon DocumentDB sin servidor

Con Amazon DocumentDB sin servidor, los clústeres son intercambiables por clústeres aprovisionados. Puede tener clústeres donde algunas instancias utilicen la tecnología sin servidor y algunas instancias estén aprovisionadas.

Compruebe que la región y la versión del motor que desee sean compatibles con DocumentDB sin servidor. Consulte Requisitos y limitaciones de DocumentDB sin servidor.

Para crear un clúster de Amazon DocumentDB en el que pueda añadir instancias sin servidor, siga el mismo procedimiento que en Creación de un clúster de Amazon DocumentDB. La única diferencia es que también debe proporcionarse el argumento `ServerlessV2ScalingConfiguration`.

El argumento `ServerlessV2ScalingConfiguration` especifica el rango de capacidad de escalado de las instancias de DocumentDB sin servidor. Se compone de los valores mínimos y máximos de la unidad de capacidad de DocumentDB (DCU) que se aplican a todas las instancias de DocumentDB sin servidor en el clúster:

- El valor de `MinCapacity` especifica la capacidad de escalado mínima.
- El valor de `MaxCapacity` especifica la capacidad de escalado máxima.

Para obtener más información sobre el escalado, consulte Configuración de escalado de Amazon DocumentDB sin servidor.

Using the Consola de administración de AWS

El siguiente ejemplo Consola de administración de AWS de configuración muestra cómo crear un clúster sin servidor de DocumentDB.

1. Inicie sesión en la Consola de administración de AWS de Amazon DocumentDB y ábrala.
2. En el panel de navegación, seleccione Clusters (Clústeres).

   > **Tip**
   >
   > Si no ve el panel de navegación del lado izquierdo de la pantalla, seleccione el icono de menú
   > (≡)
   > en la esquina superior izquierda de la página.

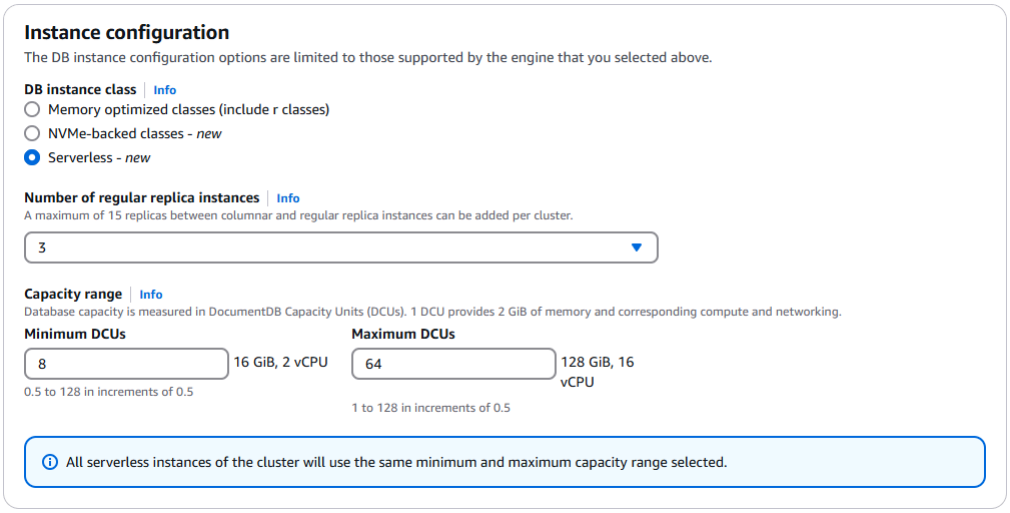
   Aparece la tabla Clústeres.
3. Seleccione Crear.

   Aparece la página Crear clúster de Amazon DocumentDB.

4. En la página Crear clúster de Amazon DocumentDB, en la sección Tipo de clúster, elija Clúster basado en instancias (esta es la opción predeterminada).
5. En la sección Configuración de clúster:
   a. En el campo Identificador del clúster, ingrese un nombre único, como **`myserverlesscluster`**. Tenga en cuenta que la consola cambiará todos los nombres de los clústeres a minúsculas independientemente de cómo se ingresen.
   b. En Versión del motor, elija 5.0.0 (es la opción predeterminada).
6. En la sección Configuración del almacenamiento en clúster, elija Amazon DocumentDB estándar (es la opción predeterminada).

> **Note**
>
> La otra opción de esta categoría es Amazon DocumentDB optimizado para E/S. Para obtener más información sobre las opciones, consulte Configuraciones de almacenamiento en clústeres de Amazon DocumentDB.

7. Sección de Configuración de instancias:
   a. En Clase de instancia de base de datos, elija Sin servidor.
   b. En Número de instancias de réplica normales, elija 3 (es la opción predeterminada).
   c. En la sección Rango de capacidad, deje los valores predeterminados para Mínimo DCUs y Máximo. DCUs Para obtener información sobre la configuración de estos parámetros, consulte Límites de instancias de Amazon DocumentDB sin servidor.



8. En la sección Conectividad, deje la configuración predeterminada de No conectarse a un recurso EC2 informático.
9. En la sección Autenticación, ingrese un nombre de usuario para el usuario principal y, a continuación, elija Autoadministrado. Ingrese una contraseña y, a continuación, confírmela.

   Si, en lugar de eso, seleccionaste Administrado en AWS Secrets Manager, consulta Administración de contraseñas con Amazon DocumentDB y AWS Secrets Manager para obtener más información.
10. Deje todas las demás opciones en sus valores predeterminados y seleccione Crear clúster.

Using the AWS CLI

En el siguiente ejemplo, sustituya cada uno *user input placeholder* por su propia información o parámetros de configuración.

Para crear un clúster compatible con las instancias sin servidor de DocumentDB mediante el AWS CLI, consulte. Creación de un clúster mediante AWS CLI

Incluya los siguientes parámetros adicionales en su comando `create-db-cluster`:

```
--serverless-v2-scaling-configuration
     MinCapacity=minimum_capacity,MaxCapacity=maximum_capacity
```

Ejemplo:

```
aws docdb create-db-cluster \
      --db-cluster-identifier sample-cluster \
      --engine docdb \
      --engine-version 5.0.0 \
      --serverless-v2-scaling-configuration MinCapacity=0.5,MaxCapacity=16 \
      --master-username user-name \
      --master-user-password password
```

Añadido de una instancia de Amazon DocumentDB sin servidor

Para añadir una instancia de DocumentDB sin servidor, siga el mismo procedimiento indicado en Agregación de una instancia de Amazon DocumentDB a un clúster y asegúrese de especificar db.serverless como clase de instancia.

Añadido de una instancia sin servidor mediante la Consola de administración de AWS

Para añadir instancias de DocumentDB sin servidor mediante la consola, consulte Agregación de una instancia de Amazon DocumentDB a un clúster y seleccione la pestaña Uso de la Consola de administración de AWS.

Agregar una instancia sin servidor mediante el AWS CLI

Para añadir instancias sin servidor de DocumentDB mediante la AWS CLI, consulte Agregación de una instancia de Amazon DocumentDB a un clúster y seleccione la pestaña Uso de. AWS CLI

Use el siguiente argumento de la CLI para la clase de instancia:

```
--db-instance-class db.serverless
```

Ejemplo:

```
aws docdb create-db-instance \
      --db-cluster-identifier sample-cluster \
      --db-instance-identifier sample-instance \
      --db-instance-class db.serverless \
      --engine docdb
```

Migración a Amazon DocumentDB sin servidor

Temas

- Migración de los clústeres de DocumentDB existentes a sistemas sin servidor
- Migración de MongoDB a DocumentDB sin servidor

Migración de los clústeres de DocumentDB existentes a sistemas sin servidor

Actualización de la versión del motor de un clúster

Si el clúster aprovisionado ejecuta una versión de motor inferior que no admite DocumentDB sin servidor, primero debe actualizar el clúster a una versión de motor compatible. Para obtener más información, consulte Actualización local de la versión principal Amazon DocumentDB.

Migración de un clúster aprovisionado a DocumentDB sin servidor

Para cambiar un clúster aprovisionado para que utilice DocumentDB sin servidor, siga estos pasos:

1. Compruebe si es preciso actualizar la versión del motor del clúster aprovisionado para usarla con DocumentDB sin servidor. Consulte Requisitos y limitaciones de DocumentDB sin servidor.

   > **Note**
   >
   > Si el clúster aprovisionado ejecuta una versión de motor que no está disponible para DocumentDB sin servidor, actualice la versión del motor del clúster: Consulte Actualización local de la versión principal Amazon DocumentDB.

2. Defina la configuración de escalado del clúster. Para obtener más información sobre cómo elegir la configuración de escalado, consulte Selección del rango de capacidad de escalado para un clúster de DocumentDB sin servidor. Para modificar la configuración de escalado de un clúster, consulte Visualización y modificación de la configuración del rango de capacidad de escalado de un clúster.
3. Configure cualquier otra propiedad del clúster para tener en cuenta los requisitos y las limitaciones de DocumentDB sin servidor de Requisitos y limitaciones de DocumentDB sin servidor.
4. Añada una o varias instancias de DocumentDB sin servidor al clúster. Siga el procedimiento indicado en Añadido de una instancia de Amazon DocumentDB sin servidor.

   > **Note**
   >
   > En algunos casos, es posible que ya tenga una o más instancias de lectura aprovisionadas en el clúster. De ser así, puede optar por convertir uno de los lectores en una instancia de DocumentDB sin servidor en lugar de crear una nueva instancia. Para ello, siga el procedimiento en Cambio de la clase de una instancia.

5. (Opcional) Realice una operación de conmutación por error para convertir una instancia de DocumentDB sin servidor en un clúster de escritura. Consulte Conmutación por error a Amazon DocumentDB.
6. (Opcional) Convierta las instancias de Amazon DocumentDB aprovisionadas en instancias de DocumentDB sin servidor (consulte Cambio de la clase de una instancia) o elimínelas del clúster (consulte Eliminación de una instancia de Amazon DocumentDB).

Using the Consola de administración de AWS

El siguiente ejemplo de Consola de administración de AWS configuración muestra el proceso de migración mediante un clúster aprovisionado de Amazon DocumentDB que ejecuta Amazon DocumentDB 5.0.0, que no requiere una actualización de la versión del motor para empezar a utilizar DocumentDB serverless. El clúster se denomina `sample` y comienza con tres instancias aprovisionadas llamadas `sample`, `sample2` y `sample3`. En este ejemplo, estas tres instancias se sustituirán por tres instancias sin servidor.

1. Inicie sesión en la Consola de administración de AWS de Amazon DocumentDB y ábrala.
2. En el panel de navegación, seleccione Clusters (Clústeres).

   > **Tip**
   >
   > Si no ve el panel de navegación del lado izquierdo de la pantalla, seleccione el icono de menú
   > (≡)
   > en la esquina superior izquierda de la página.

   Aparece la tabla Clústeres.
3. En la tabla Clústeres, seleccione la casilla de verificación del clúster al que desea añadir una instancia sin servidor.
4. Elija Actions (Acciones) y después Add instances (Añadir instancias).
5. En el cuadro de diálogo Añadir instancias, seleccione Sin servidor en la sección Clase de instancias de base de datos para cada nueva instancia sin servidor que desee crear.
6. En Ajustes de capacidad sin servidor, defina la configuración de escalado en función de la descripción de la capacidad del cuadro de diálogo.
7. (Opcional) Para añadir otra instancia, elija Añadir instancia. Siga añadiendo instancias hasta alcanzar el número deseado de instancias nuevas.

   En este ejemplo, se crean tres nuevas instancias sin servidor.
8. Seleccione Crear.

   La creación de una instancia puede tardar varios minutos. Puede usar la consola o la para ver el estado de la instancia AWS CLI . Para obtener más información, consulte Supervisión del estado de un clúster de Amazon DocumentDB.

9. Volviendo a la tabla Clústeres, seleccione las casillas de verificación de las tres instancias aprovisionadas originales.
10. Elija Acciones y, a continuación, elija Eliminar.

Durante la eliminación, se realiza automáticamente una conmutación por error para convertir a una de las instancias restantes en la instancia de escritura. Transcurridos unos minutos, se completa el proceso de eliminación. El clúster existente ahora contiene tres instancias de DocumentDB sin servidor (tal y como se define en la columna Tamaño).

Using the AWS CLI

El siguiente ejemplo de AWS CLI configuración muestra el proceso de migración mediante un clúster aprovisionado de Amazon DocumentDB que ejecuta Amazon DocumentDB 5.0.0, que no requiere una actualización de la versión del motor para empezar a utilizar DocumentDB serverless. El clúster se denomina `sample` y comienza con tres instancias aprovisionadas llamadas `sample`, `sample2` y `sample3`. En este ejemplo, estas tres instancias se sustituirán por tres instancias sin servidor. El clúster comienza se llama `sample-cluster` y empieza con dos instancias aprovisionadas llamadas `sample-provisioned-instance-1` y `sample-provisioned-instance-2`, una instancia de escritura y una de lectura.

En el siguiente ejemplo, sustituya cada uno por su propia información o *`user input placeholder`* parámetros de configuración.

Utilice `aws docdb describe-db-clusters` para determinar el estado de un clúster. El siguiente código busca el estado del clúster `sample-cluster` y muestra los resultados en una tabla:

```
aws docdb describe-db-clusters \
    --db-cluster-identifier sample-cluster \
    --query 'DBClusters[*].DBClusterMembers' \
    --output table
```

```
-------------------------------------------------------------------------------------------
|                                        DescribeDBClusters
                  |
+---------------------------------+---------------------------------
+------------------+----------------+
|  DBClusterParameterGroupStatus |      DBInstanceIdentifier       | IsClusterWriter
  | PromotionTier  |
```

```
+--------------------------------+--------------------------------
+------------------+----------------+
|  in-sync                       |  sample-provisioned-instance-2  |  False
  |  1             |
|  in-sync                       |  sample-provisioned-instance-1  |  True
  |  1             |
+--------------------------------+--------------------------------
+------------------+----------------+
```

Añada la configuración de escalado del clúster:

```
aws docdb modify-db-cluster \
    --db-cluster-identifier sample-cluster \
    --serverless-v2-scaling-configuration MinCapacity=0.5,MaxCapacity=16
```

Añada las instancias sin servidor. En este ejemplo, se añaden las nuevas instancias sin servidor denominadas `sample-serverless-instance-1` y `sample-serverless-instance-2`:

```
aws docdb create-db-instance \
    --db-cluster-identifier sample-cluster \
    --db-instance-identifier sample-serverless-instance-1 \
    --db-instance-class db.serverless \
    --engine docdb

aws docdb create-db-instance \
    --db-cluster-identifier sample-cluster \
    --db-instance-identifier sample-serverless-instance-2 \
    --db-instance-class db.serverless \
    --engine docdb
```

Introduzca lo siguiente para esperar a que las instancias sin servidor estén disponibles antes de continuar:

```
aws docdb wait db-instance-available \
    --db-instance-identifier sample-serverless-instance-1

aws docdb wait db-instance-available \
    --db-instance-identifier sample-serverless-instance-2
```

Realice una conmutación por error para que la nueva instancia de `sample-serverless-instance-1` sea el nuevo clúster de escritura:

```
aws docdb failover-db-cluster \
    --db-cluster-identifier sample-cluster \
    --target-db-instance-identifier sample-serverless-instance-1
```

La conmutación por error tarda unos segundos en completarse, tras lo cual sample-serverless-instance -1 pasa a ser el grabador del clúster. Verifíquelo con la siguiente entrada:

```
aws docdb describe-db-clusters \
    --db-cluster-identifier sample-cluster \
    --query 'DBClusters[*].DBClusterMembers' \
    --output table
```

```
-------------------------------------------------------------------------------------------------
|                                          DescribeDBClusters
                  |
+---------------------------------+---------------------------------
+------------------+----------------+
|  DBClusterParameterGroupStatus |      DBInstanceIdentifier       | IsClusterWriter
  | PromotionTier  |
+---------------------------------+---------------------------------
+------------------+----------------+
|  in-sync                       |  sample-provisioned-instance-2  |  False
  |  1             |
|  in-sync                       |  sample-provisioned-instance-1  |  False
  |  1             |
|  in-sync                       |  sample-serverless-instance-2   |  False
  |  1             |
|  in-sync                       |  sample-serverless-instance-1   |  True
  |  1             |
+---------------------------------+---------------------------------
+------------------+----------------+
```

Por último, elimine las instancias aprovisionadas originales:

```
aws docdb delete-db-instance \
    --db-instance-identifier sample-provisioned-instance-1

aws docdb delete-db-instance \
    --db-instance-identifier sample-provisioned-instance-2
```

Migración de MongoDB a DocumentDB sin servidor

Puede migrar sus bases de datos de MongoDB a DocumentDB sin servidor, igual que con elementos de Amazon DocumentDB aprovisionados. Para obtener más información, consulte Migración a Amazon DocumentDB.

Administración de Amazon DocumentDB sin servidor

Visualización y modificación de la configuración del rango de capacidad de escalado de un clúster

El argumento `ServerlessV2ScalingConfiguration` especifica el rango de capacidad de escalado de las instancias de DocumentDB sin servidor. Se compone de los valores mínimos y máximos de la unidad de capacidad de DocumentDB (DCU) que se aplican a todas las instancias de DocumentDB sin servidor en el clúster.

- **`MinCapacity`**: la capacidad de escalado mínima de cualquier instancia de DocumentDB sin servidor del clúster.
- **`MaxCapacity`**: la capacidad de escalado máxima de cualquier instancia de DocumentDB sin servidor del clúster.

> **Note**
>
> Las siguientes modificaciones de la configuración de escalado requieren el reinicio de la instancia para reflejar los nuevos valores de `MinCapacity` y `MaxCapacity`:
>
> - Cualquier cambio en el valor de `MaxCapacity`
> - Cambio en el valor de `MinCapacity` a 1.0 o inferior desde un valor superior
> - Cambio en el valor de `MinCapacity` a más de 1.0 desde un valor inferior

Para obtener más información sobre la configuración del escalado y sobre cómo seleccionar los límites de capacidad de escalado adecuados, consulte Configuración de escalado de Amazon DocumentDB sin servidor.

Using the Consola de administración de AWS

El siguiente ejemplo Consola de administración de AWS de configuración muestra cómo ver y editar los ajustes de configuración de escalado de un clúster sin servidor de DocumentDB.

1. Inicie sesión en la Consola de administración de AWS de Amazon DocumentDB y ábrala.
2. En el panel de navegación, seleccione Clusters (Clústeres).

   > **Tip**
   >
   > Si no ve el panel de navegación del lado izquierdo de la pantalla, seleccione el icono de menú
   > (≡)
   > en la esquina superior izquierda de la página.

   Aparece la tabla Clústeres.
3. En la tabla Clústeres, seleccione la casilla de verificación del clúster en el que desee modificar la capacidad de escalado.
4. Elija Actions (Acciones) y después Modify (Modificar).

   Aparece el cuadro de diálogo Modificar clúster.
5. Localice la sección Configuración de la capacidad sin servidor y establezca la configuración de escalado (Rango de capacidad) en función de la descripción de la capacidad del cuadro de diálogo.

   Para obtener más información acerca de los rangos de capacidad y el escalado, consulte Configuración de escalado de Amazon DocumentDB sin servidor.
6. Elija Continuar.
7. En Programación de modificaciones, elija Aplicar inmediatamente.
8. Elija Modificar clúster.
9. Una vez completada la modificación, se debe reiniciar cada instancia sin servidor. Para minimizar la falta de disponibilidad del escritor, realice la siguiente secuencia de operaciones:

   a. Reinicie cada instancia de lectura sin servidor.

      i. Seleccione la instancia de lectura, elija Acciones y, a continuación, Reiniciar.

ii. Espere a que el estado de la instancia vuelva a Disponible.

b. Realice una conmutación por error en una instancia sin servidor reiniciada.

i. Seleccione el clúster, elija Acciones y, a continuación, Conmutación por error.

ii. Espere a que se complete la operación de conmutación por error.

c. Reinicie la instancia sin servidor restante.

i. Seleccione la instancia restante, elija Acciones y, a continuación, Reiniciar.

ii. Espere a que el estado de la instancia vuelva a Disponible.

Using the AWS CLI

El siguiente ejemplo AWS CLI de configuración muestra la configuración de escalado actual.

En el siguiente ejemplo, sustituya cada uno *`user input placeholder`* por su propia información o parámetros de configuración.

La configuración de escalado actual del clúster se puede ver mediante el `describe-db-clusters` AWS CLI comando:

```
aws docdb describe-db-clusters \
    --db-cluster-identifier sample-cluster \
    --query 'DBClusters[0].ServerlessV2ScalingConfiguration'
```

A continuación se muestra la salida de este comando:

```
{
    "MinCapacity": 0.5,
    "MaxCapacity": 16.0
}
```

La configuración de escalado del clúster se puede modificar mediante el comando `modify-db-cluster`:

```
aws docdb modify-db-cluster \
    --db-cluster-identifier sample-cluster \
    --serverless-v2-scaling-configuration MinCapacity=0.5,MaxCapacity=32
```

Una vez completada, se debe reiniciar cada instancia sin servidor. Para minimizar la falta de disponibilidad del escritor, se puede realizar la siguiente secuencia de operaciones:

```
aws docdb reboot-db-instance \
    --db-instance-identifier sample-serverless-instance-reader

aws docdb wait db-instance-available \
    --db-instance-identifier sample-serverless-instance-reader

aws docdb failover-db-cluster \
   --db-cluster-identifier sample-cluster \
   --target-db-instance-identifier sample-serverless-instance-reader

aws docdb reboot-db-instance \
    --db-instance-identifier sample-serverless-instance-writer

aws docdb wait db-instance-available \
    --db-instance-identifier sample-serverless-instance-writer

aws docdb failover-db-cluster \
   --db-cluster-identifier sample-cluster \
   --target-db-instance-identifier sample-serverless-instance-writer
```

Visualización y modificación del nivel de promoción de los lectores sin servidor

En el caso de clústeres que incluyen múltiples instancias DocumentDB sin servidor o una combinación de instancias sin servidor y aprovisionadas, preste atención a la configuración del nivel de promoción para cada instancia sin servidor. Esta configuración controla más comportamiento para instancias sin servidor que para instancias aprovisionadas.

En el caso de las instancias aprovisionadas, la elección de nivel 0 a 15 determina únicamente el orden en que Amazon DocumentDB elige qué instancia de lectura debe promocionarse al escritor durante una operación de conmutación por error. Sin embargo, para las instancias sin servidor, el número de nivel también determina si la instancia se escala verticalmente para adaptarse a la capacidad de la instancia de escritura o si se escala independientemente en función de su propia carga de trabajo. Las instancias de lectura sin servidor de nivel 0 o 1 se mantienen con una capacidad mínima al menos igual a la de la instancia de escritura. De esta forma, quedan listas para tomar el relevo de la instancia de escritura en caso de conmutación por error. Si la instancia de

escritura es una instancia aprovisionada, Amazon DocumentDB estima la capacidad equivalente de DocumentDB sin servidor. Utilice esa estimación como capacidad mínima para la instancia de lectura sin servidor.

Las instancias de lectura de DocumentDB sin servidor de los niveles 2 a 15 no tienen la misma restricción en cuanto a capacidad mínima. Cuando están inactivas, pueden reducirse verticalmente hasta el valor mínimo de la unidad de capacidad de DocumentDB (DCU) especificado en el rango de capacidad del clúster.

Using the Consola de administración de AWS

El siguiente ejemplo Consola de administración de AWS de configuración muestra cómo ver y modificar la configuración del nivel promocional de un lector de instancias sin servidor de DocumentDB.

1. Inicie sesión en la Consola de administración de AWS de Amazon DocumentDB y ábrala.

   Los niveles de promoción de cada instancia se muestran en la columna Nivel de promoción de la Consola de administración de AWS.
2. En el panel de navegación, seleccione Clusters (Clústeres).

   > **Tip**
   >
   > Si no ve el panel de navegación del lado izquierdo de la pantalla, seleccione el icono de menú
   > (≡)
   > en la esquina superior izquierda de la página.

   Aparece la tabla Clústeres.
3. En la tabla Clústeres, seleccione la casilla de verificación de la instancia en la que desee modificar el nivel de promoción.
4. Elija Actions (Acciones) y después Modify (Modificar).

   Aparece el cuadro de diálogo Modificar instancia.
5. Localice la sección Conmutación por error y defina el Nivel de promoción en el nivel deseado.
6. Elija Continuar.
7. En Programación de modificaciones, elija Aplicar inmediatamente.

8. Elija Modificar instancia.

Using the AWS CLI

El siguiente ejemplo AWS CLI de configuración muestra la configuración de escalado actual.

En el siguiente ejemplo, sustituya cada uno *user input placeholder* por su propia información o parámetros de configuración.

Los niveles de promoción de todas las instancias de un clúster se pueden ver con el `describe-db-clusters` AWS CLI comando:

```
aws docdb describe-db-clusters \
    --db-cluster-identifier sample-cluster \
    --query 'DBClusters[0].DBClusterMembers' \
    --output table
```

A continuación se muestra la salida de este comando:

```
-------------------------------------------------------------------------------------------------
|                                          DescribeDBClusters
                  |
+---------------------------------+---------------------------------
+------------------+----------------+
|  DBClusterParameterGroupStatus |      DBInstanceIdentifier       | IsClusterWriter
  | PromotionTier  |
+---------------------------------+---------------------------------
+------------------+----------------+
|  in-sync                       |  sample-serverless-instance-2   |  False
  |  1             |
|  in-sync                       |  sample-serverless-instance-1   |  True
  |  1             |
+---------------------------------+---------------------------------
+------------------+----------------+
```

El nivel de promoción de una instancia específica se puede modificar mediante el comando `modify-db-instance`:

```
aws docdb modify-db-instance \
    --db-instance-identifier sample-serverless-instance-2 \
    --promotion-tier 3
```

Límites de instancias de Amazon DocumentDB sin servidor

Para las instancias de DocumentDB sin servidor, los siguientes límites por instancia dependen de la capacidad de escalado actual de la instancia:

- Memoria de la instancia (GiB)
- Conexiones (todas)
- Límite del cursor
- Transacciones abiertas
- Conexiones (activas)

En las siguientes tablas, se describe cómo se reducen horizontalmente los límites por instancia de las instancias sin servidor en relación con la capacidad de escalado actual de la instancia.

Tenga en cuenta que los valores límite son diferentes en función de si la configuración de escalado de `MinCapacity` del clúster se configuró en más de dos (2). Si `MinCapacity` se establece en un valor inferior o igual a 2, los valores límite para el límite del cursor, las transacciones abiertas y las conexiones (activas) se restringen a un valor máximo inferior. (El motivo técnico del límite es permitir la reducción vertical a un estado «inactivo». Para obtener más información, consulte Estado inactivo (0,5) DCUs.

Los límites de instancia db.serverless son ≤1 MinCapacity

Capacidad actual (DCU)	Memoria de la instancia (GiB)	Conexiones (todas)	Límite del cursor	Transacciones abiertas	Conexiones (activas)
0,5	1	250	6	12	39
1	2	500	12	24	79
2	4	1 000	24	48	173
4	8	2000	48	96	416
8	16	4000	96	192	1071
16	32	8000	132	264	1550

Capacidad actual (DCU)	Memoria de la instancia (GiB)	Conexiones (todas)	Límite del cursor	Transacciones abiertas	Conexiones (activas)
32	64	16 000	132	264	1550
64	128	32000	132	264	1550
128	256	60000	132	264	1550
256	512	60000	132	264	1550

Los límites de instancia db.serverless son superiores a 1 MinCapacity

Capacidad actual (DCU)	Memoria de la instancia (GiB)	Conexiones (todas)	Límite del cursor	Transacciones abiertas	Conexiones (activas)
1.5	3	7250	18	36	124
2	4	1 000	24	48	173
4	8	2000	48	96	416
8	16	4000	96	192	1071
16	32	8000	192	384	2709
32	64	16 000	384	768	4500
64	128	32000	768	1536	4500
128	256	60000	1536	3072	4500
256	512	60000	3072	6144	4500

Puede monitorear y emitir alarmas sobre los límites por instancia mediante las siguientes CloudWatch métricas. Para obtener más información sobre las CloudWatch métricas de Amazon DocumentDB, consulte. Supervisión de Amazon DocumentDB con CloudWatch

Recurso	CloudWatch métrica límite	CloudWatch métrica de uso (1 minuto como máximo)	CloudWatch métrica de uso
Memoria de la instancia	-	-	FreeableMemory
Conexiones (todas)	DatabaseConnectionsLimit	DatabaseConnectionsMax	DatabaseConnections
Cursores	DatabaseCursorsLimit	DatabaseCursorsMax	DatabaseCursors
Transacciones	TransactionsOpenLimit	TransactionsOpenMax	TransactionsOpen

Configuración de escalado de Amazon DocumentDB sin servidor

Temas

- Selección del rango de capacidad de escalado para un clúster de DocumentDB sin servidor
- Elección de la configuración MinCapacity para un clúster de DocumentDB sin servidor
- Elección de la configuración MaxCapacity para un clúster de DocumentDB sin servidor
- Evitar errores out-of-memory
- ¿Por qué no se reduce verticalmente mi instancia sin servidor?

Selección del rango de capacidad de escalado para un clúster de DocumentDB sin servidor

Antes de añadir una instancia de DocumentDB sin servidor a un clúster de Amazon DocumentDB, el clúster también debe tener el conjunto de parámetros `ServerlessV2ScalingConfiguration`.

El parámetro `ServerlessV2ScalingConfiguration` consta de dos valores que definen el rango de capacidad de escalado sin servidor de cualquier instancia sin servidor del clúster:

- **`MinCapacity`**: la capacidad de escalado mínima de cualquier instancia de DocumentDB sin servidor del clúster.

- **`MaxCapacity`**: la capacidad de escalado máxima de cualquier instancia de DocumentDB sin servidor del clúster.

Elección de la configuración **`MinCapacity`** para un clúster de DocumentDB sin servidor

Es tentador elegir siempre 0,5 para la `MinCapacity`. Este valor permite que la instancia se reduzca verticalmente a la capacidad mínima cuando esté completamente inactiva y, al mismo tiempo, permanezca activa. No obstante, en función de cómo se utilice ese clúster y de los demás ajustes que se configuren, un capacidad mínima diferente podría ser lo más efectivo. Debe tener en cuenta los factores siguientes al elegir la configuración de capacidad mínima:

- La tasa de escalado de una instancia de DocumentDB sin servidor depende de su capacidad actual. Cuanto mayor sea la capacidad actual, más rápido podrá ampliarse. Si necesita que la instancia se escale verticalmente de manera rápida a una capacidad muy alta, piense en establecer la capacidad mínima en un valor en el que la tasa de escalado cumpla con sus requisitos.
- Si normalmente modifica la clase de instancia de sus instancias en previsión de una carga de trabajo especialmente alta o baja, puede aprovechar esa experiencia para hacer una estimación aproximada del rango de capacidad de DocumentDB sin servidor equivalente. Para determinar el tamaño de la memoria de una instancia de Amazon DocumentDB aprovisionada, consulte Límites de instancias.

  Por ejemplo, supongamos que utiliza la clase de instancia `db.r6g.xlarge` cuando el clúster tiene una carga de trabajo baja. Esta clase de instancia tiene 32 GiB de memoria. Por lo tanto, puede especificar una `MinCapacity` de 16 para configurar una instancia sin servidor que pueda reducir verticalmente hasta casi la misma capacidad. Esto se debe a que cada DCU corresponde a aproximadamente 2 GiB de memoria. Podría especificar un valor algo inferior para permitir que la instancia se reduzca verticalmente aún más en caso de que la instancia de `db.r6g.xlarge` se haya infrautilizado a veces.
- Si la aplicación funciona de la manera más eficiente cuando las instancias tienen cierta cantidad de datos en la memoria caché del búfer, piense en especificar una configuración mínima de DCU en la que la memoria sea lo suficientemente grande como para contener los datos a los que se accede con frecuencia. De lo contrario, algunos datos se expulsan de la memoria caché del búfer cuando las instancias sin servidor se reducen verticalmente a un tamaño de memoria inferior. Luego, cuando las instancias se escalan de nuevo, la información se vuelve a leer en la caché del

búfer a lo largo del tiempo. Si la cantidad necesaria I/O para devolver los datos a la memoria caché del búfer es considerable, podría ser más eficaz elegir un valor mínimo de DCU más alto. Para obtener más información, consulte Determinación del tamaño de las instancias.

- Si las instancias de DocumentDB sin servidor se ejecutan la mayor parte del tiempo en una capacidad determinada, considere especificar una configuración de capacidad mínima inferior a esa línea de base, pero no muy inferior. Las instancias sin servidor pueden estimar de la manera más eficaz cuánto y con qué rapidez deben escalarse verticalmente cuando la capacidad actual no es drásticamente inferior a la capacidad requerida.
- Si la carga de trabajo aprovisionada tiene requisitos de memoria demasiado altos para clases de instancias pequeñas como T3 o T4g, elija una configuración de DCU mínima que proporcione memoria comparable a una instancia R5 o R6g.
- En particular, recomendamos la siguiente `MinCapacity` mínima de uso con las características especificadas (estas recomendaciones están sujetas a cambios):
  - Performance Insights — 2 DCUs
- En Amazon DocumentDB, la replicación se produce en la capa de almacenamiento, por lo que la capacidad del lector no afecta directamente a la replicación. Sin embargo, en el caso de las instancias de lectura de DocumentDB sin servidor que se escalan de forma independiente, asegúrese de que la capacidad mínima sea suficiente para gestionar las cargas de trabajo durante los períodos de escritura intensiva a fin de evitar la latencia de las consultas. Si las instancias de lectura en los niveles de promoción 2 a 15 experimentan problemas de rendimiento, considere aumentar la capacidad mínima del clúster. Para obtener más información sobre cómo cambiar si las instancias de lectura se escalan junto con el escritor o de manera independiente, consulte Visualización y modificación del nivel de promoción de los lectores sin servidor.

  Si tiene un clúster con instancias de lectura de DocumentDB sin servidor, los lectores no se escalan junto con la instancia de escritura cuando el nivel de promoción de los lectores no es 0 ni 1. En ese caso, establecer una capacidad mínima baja puede provocar un retraso excesivo de la replicación. Esto se debe a que es posible que los lectores no tengan la capacidad suficiente para aplicar cambios de escritura cuando la base de datos esté ocupada. Se recomienda establecer la capacidad mínima en un valor que represente una cantidad de memoria y CPU comparables con la de la instancia de escritura.
- El tiempo que tarda una instancia de DocumentDB sin servidor en escalar desde su capacidad mínima hasta su capacidad máxima depende de la diferencia entre sus valores de DCU mínima y máxima. Cuando la capacidad actual de la instancia es grande, DocumentDB sin servidor se escala verticalmente en incrementos mayores que cuando la instancia comienza desde una capacidad pequeña. Por lo tanto, si especifica una capacidad máxima relativamente grande

y la instancia está la mayor parte del tiempo cerca de esa capacidad, considere aumentar la configuración mínima de DCU. De esta forma, una instancia inactiva podrá escalar de nuevo hasta la máxima capacidad más rápidamente.

- Algunos límites de instancia vienen determinados por la capacidad actual de la instancia sin servidor, como el límite de conexiones, el límite de cursores y el límite de transacciones abiertas. Si la capacidad actual de la instancia es pequeña, los límites también serán, en consecuencia, pequeños. Si estos límites son un problema cuando la instancia sin servidor se reduce a su valor de `MinCapacity`, considere la posibilidad de aumentar la `MinCapacity` a un valor más alto. Para obtener más información, consulte Límites de instancias de Amazon DocumentDB sin servidor.
- Además, algunos límites de instancias se limitan a un valor máximo inferior si `MinCapacity` se establece en un valor inferior o igual a 1,0 DCUs, como el límite de conexiones activas, el límite de cursores y el límite de transacciones abiertas. Si estos límites máximos no son suficientes para su carga de trabajo, utilice un `MinCapacity` valor de 1,5 como mínimo DCUs. Para obtener más información, consulte Límites de instancias de Amazon DocumentDB sin servidor.

Para obtener instrucciones sobre cómo modificar la configuración de escalado de un clúster, consulte Administración de Amazon DocumentDB sin servidor.

Elección de la configuración **`MaxCapacity`** para un clúster de DocumentDB sin servidor

Es tentador elegir siempre un valor alto para la configuración de capacidad máxima de DocumentDB sin servidor. Una alta capacidad máxima permite que la instancia se escale verticalmente cuando ejecuta una carga de trabajo intensiva. Un valor bajo evita la posibilidad de cobros inesperados. Según cómo utilice ese clúster y los demás ajustes que configure, el valor más efectivo podría ser mayor o menor de lo que pensaba originalmente. Tenga en cuenta los factores siguientes al elegir la configuración de capacidad máxima:

- La capacidad máxima debe ser al menos tan alta como la capacidad mínima. Usted puede definir la capacidad mínima y máxima para que sean idénticas. Sin embargo, en ese caso, la capacidad nunca aumenta ni baja. Por lo tanto, utilizar valores idénticos para la capacidad mínima y máxima no es apropiado fuera de situaciones de prueba.
- La capacidad máxima debe ser como mínimo de 1,0 DCUs y 256 como máximo DCUs.
- Recomendamos supervisar el escalado y el uso de recursos de las instancias sin servidor. Si su instancia sin servidor se escala con frecuencia hasta alcanzar su capacidad máxima y tiene

limitaciones de recursos (por ejemplo, cuando la métrica `DCUUtilization` es de 100,0), le recomendamos seleccionar un valor de `MaxCapacity` más alto. Para obtener más información, consulte Supervisión de Amazon DocumentDB sin servidor.

- Si normalmente modifica la clase de instancia de sus instancias aprovisionadas en previsión de una carga de trabajo especialmente alta o baja, puede aprovechar esa experiencia para hacer una estimación del rango de capacidad de DocumentDB sin servidor equivalente. Para determinar el tamaño de la memoria de las instancias de Amazon DocumentDB aprovisionadas, consulte Límites de instancias.

  Por ejemplo, supongamos que utiliza la clase de instancia `db.r6g.4xlarge` cuando el clúster tiene una carga de trabajo elevada. Esta clase de instancia tiene 128 GiB de memoria. Por lo tanto, puede especificar una configuración de DCU máxima de 64 para configurar una instancia sin servidor que pueda escalar verticalmente hasta casi la misma capacidad. Esto se debe a que cada DCU corresponde a aproximadamente 2 GiB de memoria. Puede especificar un valor algo mayor para permitir que la instancia se amplíe más en caso de que la instancia de `db.r6g.4xlarge` a veces no tenga la capacidad suficiente para gestionar la carga de trabajo de forma eficaz.
- Si tiene un límite presupuestario para usar su base de datos, elija un valor que se mantenga dentro de ese límite, incluso si todas las instancias sin servidor se ejecutan a máxima capacidad todo el tiempo. Recuerde que, cuando tenga n instancias sin servidor en el clúster, la capacidad sin servidor máxima teórica que el clúster puede consumir en cualquier momento es n veces la configuración máxima de DCU para el clúster. (La cantidad real consumida podría ser menor, por ejemplo, si algunos lectores escalan independientemente del escritor).
- Si hace uso de instancias de lectura sin servidor para descargar parte de la carga de trabajo de solo lectura de la instancia de escritura, es posible que pueda elegir una configuración de capacidad máxima inferior. Esto se hace para reflejar que cada instancia de lectura no necesita escalar tan alto como si el clúster contuviera solo una instancia.
- Supongamos que desea protegerse contra el uso excesivo por parámetros de base de datos mal configurados o consultas ineficientes en la aplicación. En ese caso, puede evitar un uso excesivo por error eligiendo un ajuste de capacidad máxima inferior al más alto absoluto que podría establecer.
- Si los picos por actividad real del usuario son poco frecuentes, pero sí ocurren, puede tener en cuenta esas ocasiones al elegir la configuración de capacidad máxima. Si la prioridad es que la aplicación siga funcionando con un rendimiento y escalabilidad completos, puede especificar una configuración de capacidad máxima superior a la observada en el uso normal. Si está bien que la aplicación se ejecute con un rendimiento reducido durante picos de actividad muy extremos, puede elegir una configuración de capacidad máxima ligeramente inferior. Asegúrese de elegir una

configuración que aún tenga suficiente memoria y recursos de CPU para mantener la aplicación en ejecución.

- Si habilita opciones de configuración en el clúster que aumenten el uso de memoria para cada instancia, tenga en cuenta esa memoria al decidir el valor máximo de DCU. Estos ajustes incluyen los de Información sobre rendimiento. Asegúrese de que el valor máximo de la DCU permite que las instancias sin servidor se escalen verticalmente lo suficiente como para gestionar la carga de trabajo cuando se usen esas características. Para obtener información sobre cómo solucionar problemas causados por la combinación de una configuración de DCU máxima baja y características de Amazon DocumentDB que impongan sobrecarga de memoria, consulte Evitar errores out-of-memory (a continuación).
- En particular, recomendamos la siguiente `MaxCapacity` mínima de uso con las características especificadas (estas recomendaciones están sujetas a cambios):
  - Creación de instancias sin servidor en un clúster con un gran volumen de datos: 2 DCUs (esto incluye la creación de instancias sin servidor como parte de la restauración de un clúster).
- Algunos límites de instancia vienen determinados por la capacidad actual de la instancia, como el límite de conexiones, el límite de cursores y el límite de transacciones abiertas. A la hora de elegir el valor de `MaxCapacity` de la carga de trabajo, asegúrese de tener en cuenta estos límites de instancia para evitar que uno de ellos se vea obstaculizado por uno de ellos. Para obtener más información, consulte Límites de instancias de Amazon DocumentDB sin servidor.

Para obtener instrucciones sobre cómo modificar la configuración de escalado de un clúster, consulte Administración de Amazon DocumentDB sin servidor.

Evitar errores out-of-memory

Si una de sus instancias de DocumentDB sin servidor alcanza constantemente el límite de su capacidad máxima, Amazon DocumentDB indica esta condición y establece la instancia en un estado de incompatible-parameters. Si bien la instancia tiene el estado incompatible-parameters, algunas operaciones quedan bloqueadas. Por ejemplo, no se puede actualizar la versión del motor. Para obtener más información sobre el estado de una instancia de Amazon DocumentDB, consulte Supervisión del estado de una instancia de Amazon DocumentDB.

Por lo general, la instancia pasa a este estado cuando se reinicia con frecuencia debido a out-of-memory errores. Amazon DocumentDB registra un evento cuando se produce este tipo de reinicio. Para ver los eventos de los recursos, consulte Visualización de eventos de Amazon DocumentDB. Los casos de uso de memoria inusualmente elevados pueden producirse debido a una sobrecarga

en el ajuste de configuraciones, como Información sobre rendimiento. También puede provenir de una carga de trabajo pesada en la instancia o de la administración de metadatos asociados a un gran número de objetos de esquema.

Si la presión de memoria disminuye para que la instancia no alcance su capacidad máxima muy a menudo, Amazon DocumentDB cambia automáticamente el estado de la instancia a disponible.

Para recuperarse de esta situación, puede llevar a cabo algunas o todas las acciones siguientes:

- Aumente el límite inferior de capacidad para instancias sin servidor. Para ello, cambie el valor mínimo de la unidad de capacidad de DocumentDB (DCU) para el clúster. Al hacerlo, se evitan problemas en los que la capacidad de una base de datos inactiva se escala a menos memoria de la necesaria para las características activadas en el clúster. Después de cambiar la configuración de DCU del clúster, reinicie la instancia sin servidor. Cuando lo hace, se evalúa si Amazon DocumentDB puede restablecer el estado de nuevo a disponible.
- Aumente el límite superior de capacidad para instancias sin servidor. Para ello, cambie el valor máximo de DCU para el clúster. Al hacerlo, se evitan problemas en los que una base de datos ocupada no puede escalar a una capacidad con suficiente memoria para las funciones activadas en el clúster y la carga de trabajo de la base de datos. Después de cambiar la configuración de DCU del clúster, reinicie la instancia sin servidor. Cuando lo hace, se evalúa si Amazon DocumentDB puede restablecer el estado de nuevo a disponible.
- Desactivar los ajustes de configuración que requieren sobrecarga de memoria. Por ejemplo, suponga que tiene activada una característica como Información sobre rendimiento, pero no la usa. Si es así, puede desactivarla. O bien, puede ajustar los valores de capacidad mínima y máxima del clúster para tener en cuenta la memoria utilizada por esos tipos de características. Para ver instrucciones sobre cómo elegir la configuración de capacidad mínima y máxima, consulte Selección del rango de capacidad de escalado para un clúster de DocumentDB sin servidor.
- Reduzca la carga de trabajo de la instancia. Por ejemplo, puede añadir instancias de lectura al clúster para distribuir la carga de las consultas de solo lectura entre más instancias.

¿Por qué no se reduce verticalmente mi instancia sin servidor?

En algunos casos, DocumentDB sin servidor no se reduce verticalmente a la capacidad mínima, incluso sin carga en la base de datos. Esto podría deberse por alguna de las siguientes razones:

- Información sobre rendimiento puede aumentar el uso de los recursos e impedir que la base de datos se reduzca verticalmente a su capacidad mínima. Estas son algunas de ellas:

- Si una instancia de lectura no se reduce verticalmente al mínimo y permanece en la misma capacidad o más que la instancia de escritura, compruebe el nivel de prioridad de la instancia de lectura. Las instancias de lectura de DocumentDB sin servidor de nivel 0 o 1 se mantienen con una capacidad mínima al menos igual a la de la instancia de escritura. Cambie el nivel de prioridad del lector a 2 o más para que se escale y se reduzca verticalmente independientemente del escritor. Para obtener más información, consulte Escalado de Amazon DocumentDB sin servidor.
- Las cargas de trabajo pesadas de las bases de datos pueden aumentar el uso de recursos.
- Los grandes volúmenes de bases de datos pueden aumentar el uso de recursos. Amazon DocumentDB utiliza recursos de memoria y CPU para la administración de clústeres. Amazon DocumentDB requiere más CPU y memoria para administrar los clústeres con volúmenes de bases de datos más grandes. Si la capacidad mínima del clúster es inferior al mínimo requerido para la administración del clúster, el clúster no se reducirá verticalmente a la capacidad mínima.
- La actividad de mantenimiento en segundo plano puede aumentar periódicamente el uso de recursos.

Si la base de datos sigue sin reducir verticalmente la capacidad mínima configurada, deténgala y reiníciela para recuperar los fragmentos de memoria que se hayan acumulado con el tiempo. Al detener e iniciar una base de datos, se produce un tiempo de inactividad, por lo que recomendamos hacerlo con moderación.

Supervisión de Amazon DocumentDB sin servidor

Para obtener más información sobre la supervisión en Amazon DocumentDB, consulte Monitorización de Amazon DocumentDB.

Temas

- Memoria insuficiente: estado de parámetros incompatibles
- CloudWatch Métricas de Amazon para DocumentDB sin servidor
- Supervisión del rendimiento de DocumentDB sin servidor con Información sobre rendimiento

Memoria insuficiente: estado de parámetros incompatibles

Si una de sus instancias sin servidor alcanza constantemente el límite de su capacidad máxima, Amazon DocumentDB indica esta condición y establece la instancia en un estado de incompatible-parameters. Para obtener más información, consulte Evitar errores out-of-memory.

CloudWatch Métricas de Amazon para DocumentDB sin servidor

Para obtener más información sobre el uso CloudWatch con Amazon DocumentDB, consulte. Supervisión de Amazon DocumentDB con CloudWatch

Puede ver sus instancias sin servidor CloudWatch para monitorear la capacidad consumida por cada instancia con la `ServerlessDatabaseCapacity` métrica. También puede supervisar todas las CloudWatch métricas estándar de DocumentDB, como `DatabaseConnections` las consultas. Para ver la lista completa de CloudWatch métricas que puede supervisar para Amazon DocumentDB, consulte. Supervisión de Amazon DocumentDB con CloudWatch Es importante monitorear las siguientes métricas a CloudWatch nivel de instancia para que pueda comprender cómo sus instancias sin servidor de DocumentDB se escalan hacia arriba y hacia abajo. Todas estas métricas se calculan cada segundo. De esta forma, puede supervisar el estado en uso de sus instancias sin servidor. Puede configurar alarmas para notificarle si alguna de las instancias sin servidor se acerca a un umbral de métricas relacionadas con la capacidad. Puede determinar si los ajustes de capacidad mínima y máxima son apropiados o si necesita ajustarlos. Puede determinar dónde debe centrar sus esfuerzos para optimizar la eficiencia de la base de datos.

- **`ServerlessDatabaseCapacity`**— Como métrica a nivel de instancia, indica el número representado por la capacidad de la instancia actual. DCUs Como métrica en el nivel de clúster, representa el promedio de los valores de `ServerlessDatabaseCapacity` de todas las instancias de DocumentDB sin servidor del clúster.
- **`DCUUtilization.`**: esta métrica es nueva en DocumentDB sin servidor. Este valor se representa como un porcentaje. Se calcula como el valor de la métrica `ServerlessDatabaseCapacity` dividida por el valor máximo de DCU del clúster. Tenga en cuenta las siguientes pautas para interpretar esta métrica y tomar medidas:
  - Si esta métrica se aproxima a un valor de `100.0`, la instancia se ha escalado verticalmente al punto máximo posible. Considere aumentar la configuración máxima de DCU para el clúster. De este modo, las instancias de escritura y lectura podrán escalarse a una mayor capacidad.
  - Supongamos que una carga de trabajo de solo lectura hace que una instancia de lectura se aproxime a un valor `DCUUtilization` de `100.0`, mientras que la instancia de escritura no está cerca de su capacidad máxima. En ese caso, considere añadir instancias de lectura adicionales al clúster. De esta forma, puede distribuir la parte de solo lectura de la carga de trabajo en más instancias, lo que reduce la carga en cada instancia de lectura.
  - Supongamos que está ejecutando una aplicación de producción, donde el rendimiento y la escalabilidad son las principales consideraciones. En este caso, puede establecer el valor máximo de DCU del clúster en un número elevado. Su objetivo es que la métrica

`DCUUtilization` quede siempre por debajo de 100,0. Con un valor de DCU máximo alto, puede estar seguro de tener suficiente espacio en caso de que haya picos inesperados en la actividad de la base de datos. Solo se le cobrará por la capacidad de base de datos que se consuma realmente.

- **`CPUUtilization`**: esta métrica se interpreta de forma diferente en DocumentDB sin servidor que en las instancias aprovisionadas. Para DocumentDB sin servidor, este valor es un porcentaje que se calcula como la cantidad de CPU que se utiliza actualmente dividida por la capacidad de CPU disponible bajo el valor máximo de DCU del clúster. Amazon DocumentDB supervisa este valor automáticamente y escala verticalmente su instancia sin servidor cuando esta utiliza sistemáticamente una elevada proporción de su capacidad de CPU.

  Si esta métrica se aproxima a un valor de `100.0`, la instancia ha alcanzado su capacidad máxima de CPU. Considere aumentar la configuración máxima de DCU para el clúster. Si esta métrica se aproxima a un valor de `100.0` en una instancia de lectura, considere añadir instancias de lectura adicionales al clúster. De esta forma, puede distribuir la parte de solo lectura de la carga de trabajo distribuida en más instancias, y así reducir la carga en cada instancia de lectura.

- **`FreeableMemory`**: este valor representa la cantidad de memoria sin utilizar que está disponible cuando la instancia de DocumentDB sin servidor se escala a su capacidad máxima. Por cada DCU en cuya capacidad actual esté por debajo de la capacidad máxima, este valor aumenta aproximadamente 2 GiB. Por lo tanto, esta métrica no se aproxima a cero hasta que la instancia se escala verticalmente al punto máximo posible.

  Si esta métrica se aproxima a un valor de cero, la instancia se ha escalado verticalmente tanto como es posible y se acerca al límite de memoria disponible. Considere aumentar la configuración máxima de DCU para el clúster. Si esta métrica se aproxima a un valor de cero en una instancia de lectura, considere añadir instancias de lectura adicionales al clúster. De esta forma, puede distribuir la parte de solo lectura de la carga de trabajo entre más instancias, y así reducir el uso de memoria en cada instancia de lectura.

- **`TempStorageIops`**: el número de IOPS realizadas en el almacenamiento local adjuntas a la instancia. Incluye las IOPS de lecturas y escrituras. Esta métrica representa un recuento y se mide una vez por segundo. Esta es una nueva métrica para DocumentDB sin servidor. Para obtener más información, consulte Supervisión de Amazon DocumentDB con CloudWatch.

- **`TempStorageThroughput`**: la cantidad de datos transferidos desde el almacenamiento local asociado a la instancia y hacia este. Esta métrica representa un número de bytes y se mide una vez por segundo. Esta es una nueva métrica para DocumentDB sin servidor. Para obtener más información, consulte Supervisión de Amazon DocumentDB con CloudWatch.

Por lo general, la mayoría de los escalados verticales a instancias de DocumentDB sin servidor se deben al uso de la memoria y la actividad de CPU. Las métricas `TempStorageIops` y `TempStorageThroughput` pueden ayudar a diagnosticar los raros casos en los que la actividad de red para transferencias entre la instancia y los dispositivos de almacenamiento locales es responsable de aumentos de capacidad no esperados. Para supervisar otra actividad de red, puede utilizar estas métricas existentes:

- `NetworkReceiveThroughput`
- `NetworkThroughput`
- `NetworkTransmitThroughput`
- `StorageNetworkReceiveThroughput`
- `StorageNetworkThroughput`
- `StorageNetworkTransmitThroughput`

Cómo se aplican las CloudWatch métricas sin servidor de DocumentDB a su factura AWS

Los cargos sin servidor de DocumentDB que figuran en su AWS factura se calculan en función de la misma `ServerlessDatabaseCapacity` métrica que puede supervisar. El mecanismo de facturación puede diferir del CloudWatch promedio calculado para esta métrica en los casos en que utilice la capacidad sin servidor de DocumentDB solo durante una parte de una hora. También puede variar si los problemas del sistema hacen que la CloudWatch métrica no esté disponible durante períodos breves. Por lo tanto, es posible que vea un valor ligeramente diferente de las horas de DCU en su factura que si computa el número usted mismo a partir del valor de `ServerlessDatabaseCapacity` promedio.

Ejemplos de comandos de Amazon CloudWatch CLI para métricas sin servidor de DocumentDB

Los siguientes AWS CLI ejemplos muestran cómo puede supervisar las CloudWatch métricas más importantes relacionadas con DocumentDB serverless. En cada caso, sustituya la cadena `Value=` para el parámetro `--dimensions` con el identificador de su propia instancia de DocumentDB sin servidor.

En el siguiente ejemplo de Linux se muestran los valores de capacidad mínima, máxima y promedio de una instancia, medidos cada 10 minutos durante 1 hora. El comando de fecha de Linux especifica

las horas de inicio y finalización en relación con la fecha y la hora en curso. La función `sort_by` en el parámetro `--query` ordena los resultados cronológicamente basándose en el campo `Timestamp`.

```
aws cloudwatch get-metric-statistics \
    --metric-name "ServerlessDatabaseCapacity" \
    --start-time "$(date -d '1 hour ago')" \
    --end-time "$(date -d 'now')" \
    --period 600 \
    --namespace "AWS/DocDB" \
    --statistics Minimum Maximum Average \
    --dimensions Name=DBInstanceIdentifier,Value=my_instance \
    --query 'sort_by(Datapoints[*].
{min:Minimum,max:Maximum,avg:Average,ts:Timestamp},&ts)' \
    --output table
```

El siguiente ejemplo de Linux muestra la supervisión de la capacidad de una instancia en un clúster. Mide el uso de capacidad mínimo, máximo y promedio de una instancia. Las mediciones se toman una vez por hora durante un período de tres horas. En estos ejemplos, se utiliza la `DCUUtilization` métrica que representa un porcentaje del límite superior DCUs, en lugar de `ServerlessDatabaseCapacity` representar un número fijo de. DCUs De esta forma, no necesita conocer los números reales de los valores de DCU mínima y máxima en el rango de capacidad. Puede ver porcentajes que oscilan entre 0 y 100.

```
aws cloudwatch get-metric-statistics \
    --metric-name "DCUUtilization" \
    --start-time "$(date -d '3 hours ago')" \
    --end-time "$(date -d 'now')" \
    --period 3600 \
    --namespace "AWS/DocDB" \
    --statistics Minimum Maximum Average \
    --dimensions Name=DBInstanceIdentifier,Value=my_instance \
    --query 'sort_by(Datapoints[*].
{min:Minimum,max:Maximum,avg:Average,ts:Timestamp},&ts)' \
    --output table
```

En el siguiente ejemplo de Linux se hacen mediciones similares a las anteriores. En este caso, las medidas corresponden a la métrica `CPUUtilization`. Las mediciones se toman cada 10 minutos durante un período de 1 hora. Los números representan el porcentaje de CPU disponible utilizada, en función de los recursos de CPU disponibles para la configuración de capacidad máxima de la instancia.

```
aws cloudwatch get-metric-statistics \
    --metric-name "CPUUtilization" \
    --start-time "$(date -d '1 hour ago')" \
    --end-time "$(date -d 'now')" \
    --period 600 \
    --namespace "AWS/DocDB" \
    --statistics Minimum Maximum Average \
    --dimensions Name=DBInstanceIdentifier,Value=my_instance \
    --query 'sort_by(Datapoints[*].
{min:Minimum,max:Maximum,avg:Average,ts:Timestamp},&ts)' \
    --output table
```

En el siguiente ejemplo de Linux se hacen mediciones similares a las anteriores. En este caso, las medidas corresponden a la métrica `FreeableMemory`. Las mediciones se toman cada 10 minutos durante un período de 1 hora.

```
aws cloudwatch get-metric-statistics \
    --metric-name "FreeableMemory" \
    --start-time "$(date -d '1 hour ago')" \
    --end-time "$(date -d 'now')" \
    --period 600 \
    --namespace "AWS/DocDB" \
    --statistics Minimum Maximum Average \
    --dimensions Name=DBInstanceIdentifier,Value=my_instance \
    --query 'sort_by(Datapoints[*].
{min:Minimum,max:Maximum,avg:Average,ts:Timestamp},&ts)' \
    --output table
```

Supervisión del rendimiento de DocumentDB sin servidor con Información sobre rendimiento

Puede utilizar Información sobre rendimiento para supervisar el rendimiento de las instancias de DocumentDB sin servidor. Para conocer los procedimientos de información del rendimiento, consulte Supervisión con información sobre rendimiento.

Los siguientes son contadores de Información sobre rendimiento nuevos aplicables a instancias de DocumentDB sin servidor:

- **`os.general.serverlessDBCapacity`**— La capacidad actual de la instancia en DCUs. El valor corresponde a la `ServerlessDatabaseCapacity` CloudWatch métrica de la instancia.

- **`os.general.dcuUtilization`**— El porcentaje de la capacidad actual respecto de la capacidad máxima configurada. El valor corresponde a la `DCUUtilization` CloudWatch métrica de la instancia.
- **`os.general.maxConfiguredDcu`**: la capacidad máxima que configuró para esta instancia de DocumentDB sin servidor. Se mide en DCUs.
- **`os.general.minConfiguredDcu`**: la capacidad mínima que configuró para esta instancia de DocumentDB sin servidor. Se mide en DCUs.

Para ver la lista completa de contadores de información de rendimiento, consulte Métricas de contador para Información sobre rendimiento.

Cuando se muestran los valores de vCPU para una instancia de DocumentDB sin servidor en la Información sobre rendimiento, estos valores representan estimaciones basadas en el valor de DCU de la instancia. En el intervalo predeterminado de un minuto, los valores fraccionarios de vCPU se redondean al número entero más cercano. En intervalos más largos, el valor de vCPU que se muestra es el promedio de los valores de vCPU enteros de cada minuto.

Desarrollo de Amazon DocumentDB

En estas secciones se explica la implementación mediante Amazon DocumentDB.

Temas

- Conexión a Amazon DocumentDB
- Programación con Amazon DocumentDB

Conexión a Amazon DocumentDB

Amazon DocumentDB ofrece varias opciones de conexión, incluidas las conexiones programáticas mediante controladores MongoDB, la conexión desde fuera de una VPC mediante túneles SSH o una VPN de AWS, y herramientas populares como Studio 3T y DataGrip. El servicio admite conexiones de conjuntos de réplicas para una alta disponibilidad. Para el análisis y la elaboración de informes, puede conectarse mediante controladores JDBC u ODBC. Las instancias de EC2 de la misma VPC pueden conectarse directamente a los clústeres de DocumentDB. Todas las conexiones requieren TLS y credenciales/autenticación de AWS adecuadas.

Temas

- Conexión mediante programación a Amazon DocumentDB
- Conexión a un clúster de Amazon DocumentDB desde fuera de una Amazon VPC
- Conexión a Amazon DocumentDB como conjunto de réplicas
- Conexión a un clúster de Amazon DocumentDB desde Studio 3T
- Conexión a Amazon DocumentDB mediante DataGrip
- Connect mediante Amazon EC2
- Conexión mediante el controlador JDBC de Amazon DocumentDB
- Conexión mediante el controlador ODBC de Amazon DocumentDB

Conexión mediante programación a Amazon DocumentDB

En esta sección, se incluyen ejemplos de código que demuestran cómo conectarse a Amazon DocumentDB (con compatibilidad con MongoDB) utilizando diferentes lenguajes. Los ejemplos se dividen en dos secciones en función de si se conecta a un clúster que tiene habilitado o deshabilitado Transport Layer Security (TLS). De manera predeterminada, TLS está habilitado para los nuevos

clústeres de Amazon DocumentDB. Sin embargo, puede desactivar TLS si lo desea. Para obtener más información, consulte Cifrado de datos en tránsito.

Si intenta conectarse a su Amazon DocumentDB desde fuera de la VPC en la que reside el clúster, consulte Conexión a un clúster de Amazon DocumentDB desde fuera de una Amazon VPC.

Antes de conectarse a su clúster, debe saber si TLS está habilitado en él. En la siguiente sección, se muestra cómo determinar el valor del parámetro `tls` del clúster mediante la Consola de administración de AWS o la AWS CLI. A continuación, puede buscar y aplicar el ejemplo de código adecuado.

Temas

- Determinación del valor del parámetro tls
- Conexión con TLS habilitado
- Conexión con TLS deshabilitado

Determinación del valor del parámetro **`tls`**

Para determinar si el clúster tiene habilitado TLS, hay que seguir un proceso de dos pasos que puede realizar mediante la Consola de administración de AWS o la AWS CLI.

1. Determine qué grupo de parámetros rige el clúster.

   Using the Consola de administración de AWS

   1. Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon DocumentDB en https://console.aws.amazon.com/docdb.
   2. En el panel de navegación izquierdo, elija Clusters (Clústeres).
   3. En la lista de clústeres, seleccione el nombre del clúster.
   4. La página resultante muestra los detalles del clúster seleccionado. Seleccione la pestaña Configuración. En la sección Configuraciones y estado, busque el nombre del grupo de parámetros debajo del Grupo de parámetros del clúster.

   Using the AWS CLI

   El siguiente código de la AWS CLI determina qué parámetro rige el clúster. Asegúrese de reemplazar *`sample-cluster`* por el nombre del clúster.

```
aws docdb describe-db-clusters \
    --db-cluster-identifier sample-cluster \
    --query 'DBClusters[*].[DBClusterIdentifier,DBClusterParameterGroup]'
```

La salida de esta operación será similar a lo que se indica a continuación:

```
[
       [
           "sample-cluster",
           "sample-parameter-group"
       ]
]
```

2. Determine el valor del parámetro **`tls`** en el grupo de parámetros del clúster.

   Using the Consola de administración de AWS

   1. En el panel de navegación, seleccione Grupos de parámetros.
   2. En la ventana Grupos de parámetros del clúster, seleccione el nombre del grupo de parámetros del clúster del Paso 1d.
   3. En la página resultante se muestran los parámetros del grupo de parámetros del clúster. Puede ver el valor del parámetro `tls` aquí. Para obtener información sobre la modificación de este parámetro, consulte Modificación de grupos de parámetros de clúster de Amazon DocumentDB.

   Using the AWS CLI

   Puede utilizar el comando de la `describe-db-cluster-parameters` AWS CLI para ver los detalles de los parámetros del grupo de parámetros del clúster.

   - **`--describe-db-cluster-parameters`** — para obtener una lista de los parámetros de un grupo de parámetros, junto con sus valores.
     - **`--db-cluster-parameter-group name`** — obligatorio. El nombre del grupo de parámetros del clúster.

   En los siguientes ejemplos, reemplace cada *`marcador de posición del usuario`* con la información de su clúster.

```
aws docdb describe-db-cluster-parameters \
    --db-cluster-parameter-group-name sample-parameter-group
```

La salida de esta operación será similar a lo que se indica a continuación:

```
{
        "Parameters": [
            {
                "ParameterName": "profiler_threshold_ms",
                "ParameterValue": "100",
                "Description": "Operations longer than profiler_threshold_ms
 will be logged",
                "Source": "system",
                "ApplyType": "dynamic",
                "DataType": "integer",
                "AllowedValues": "50-2147483646",
                "IsModifiable": true,
                "ApplyMethod": "pending-reboot"
            },
            {
                "ParameterName": "tls",
                "ParameterValue": "disabled",
                "Description": "Config to enable/disable TLS",
                "Source": "user",
                "ApplyType": "static",
                "DataType": "string",
                "AllowedValues": "disabled,enabled,fips-140-3",
                "IsModifiable": true,
                "ApplyMethod": "pending-reboot"
            }
        ]
}
```

> **Note**
>
> Amazon DocumentDB admite los puntos de conexión FIPS 140-3 a partir de los clústeres con Amazon DocumentDB 5.0 (versión del motor 3.0.3727) en las siguientes regiones: ca-central-1, us-west-2, us-east-1, us-east-2, us-gov-east-1, us-gov-west-1.

Después de determinar el valor del parámetro `tls`, continúe conectándose al clúster utilizando uno de los ejemplos de código que se muestran en las siguientes secciones.

- Conexión con TLS habilitado
- Conexión con TLS deshabilitado

Conexión con TLS habilitado

Para ver un ejemplo de código para conectarse mediante programación a un clúster de Amazon DocumentDB con TLS habilitado, elija la pestaña adecuada al lenguaje que desea utilizar.

Para cifrar datos en tránsito, descargue la clave pública para Amazon DocumentDB denominada `global-bundle.pem` mediante la siguiente operación.

```
wget https://truststore.pki.rds.amazonaws.com/global/global-bundle.pem
```

Si l aplicación está en Microsoft Windows y requiere un archivo PKCS7, puede descargar el paquete de certificados PKCS7. Este paquete contiene los certificados intermedio y raíz en https://truststore.pki.rds.amazonaws.com/global/global-bundle.p7b.

Python

El código siguiente demuestra cómo conectarse a Amazon DocumentDB utilizando Python cuando TLS está habilitado.

En el siguiente ejemplo, reemplace cada *marcador de posición del usuario* con la información de su clúster.

```
import pymongo
import sys

##Create a MongoDB client, open a connection to Amazon DocumentDB as a replica set
 and specify the read preference as secondary preferred
client = pymongo.MongoClient('mongodb://sample-user:password@sample-
cluster.node.us-east-1.docdb.amazonaws.com:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')

##Specify the database to be used
db = client.sample_database

##Specify the collection to be used
```

```
col = db.sample_collection

##Insert a single document
col.insert_one({'hello':'Amazon DocumentDB'})

##Find the document that was previously written
x = col.find_one({'hello':'Amazon DocumentDB'})

##Print the result to the screen
print(x)

##Close the connection
client.close()
```

Node.js

El código siguiente demuestra cómo conectarse a Amazon DocumentDB utilizando Node.js cuando TLS está habilitado.

> **Important**
>
> Existe una limitación conocida con los controladores de Node.js anteriores a la versión 6.13.1, ya que Amazon DocumentDB no los admite actualmente para la autenticación de identidad de IAM. Los controladores y las herramientas de Node.js que utilizan el controlador Node.js (por ejemplo, mongosh) deben actualizarse para utilizar el controlador Node.js, versión 6.13.1 o posterior.

En el siguiente ejemplo, reemplace cada *marcador de posición del usuario* con la información de su clúster.

```
var MongoClient = require('mongodb').MongoClient

//Create a MongoDB client, open a connection to DocDB; as a replica set,
//  and specify the read preference as secondary preferred

var client = MongoClient.connect(
'mongodb://sample-user:password@sample-cluster.node.us-
east-1.docdb.amazonaws.com:27017/sample-database?
tls=true&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false',
{
  tlsCAFile: `global-bundle.pem` //Specify the DocDB; cert
```

```
},
function(err, client) {
    if(err)
        throw err;

    //Specify the database to be used
    db = client.db('sample-database');

    //Specify the collection to be used
    col = db.collection('sample-collection');

    //Insert a single document
    col.insertOne({'hello':'Amazon DocumentDB'}, function(err, result){
      //Find the document that was previously written
      col.findOne({'hello':'Amazon DocumentDB'}, function(err, result){
        //Print the result to the screen
        console.log(result);

        //Close the connection
        client.close()
      });
   });
});
```

PHP

El código siguiente demuestra cómo conectarse a Amazon DocumentDB utilizando PHP cuando TLS está habilitado.

En el siguiente ejemplo, reemplace cada *marcador de posición del usuario* con la información de su clúster.

```
<?php
//Include Composer's autoloader
require 'vendor/autoload.php';

$TLS_DIR = "/home/ubuntu/global-bundle.pem";

//Create a MongoDB client and open connection to Amazon DocumentDB
$client = new MongoDB\Client("mongodb://sample-user:password@sample-cluster.node.us-
east-1.docdb.amazonaws.com:27017/?retryWrites=false", ["tls" => "true", "tlsCAFile"
 => $TLS_DIR ]);
```

```
//Specify the database and collection to be used
$col = $client->sampledatabase->samplecollection;

//Insert a single document
$result = $col->insertOne( [ 'hello' => 'Amazon DocumentDB'] );

//Find the document that was previously written
$result = $col->findOne(array('hello' => 'Amazon DocumentDB'));

//Print the result to the screen
print_r($result);
?>
```

Go

El código siguiente demuestra cómo conectarse a Amazon DocumentDB utilizando Go cuando TLS está habilitado.

> **Note**
>
> A partir de la versión 1.2.1, el controlador de MongoDB Go solo utilizará el primer certificado de servidor de CA que se encuentre en `sslcertificateauthorityfile`. El siguiente código de ejemplo corrige esta limitación anexando manualmente todos los certificados de servidor que se encuentran en `sslcertificateauthorityfile` a una configuración TLS personalizada utilizada durante la creación del cliente.

En los siguientes ejemplos, reemplace cada *`marcador de posición del usuario`* con la información de su clúster.

```
package main

import (
 "context"
 "fmt"
 "log"
 "time"

 "go.mongodb.org/mongo-driver/bson"
 "go.mongodb.org/mongo-driver/mongo"
 "go.mongodb.org/mongo-driver/mongo/options"
```

```
 "io/ioutil"
 "crypto/tls"
 "crypto/x509"
 "errors"
)

const (
 // Path to the AWS CA file
 caFilePath = "global-bundle.pem"

 // Timeout operations after N seconds
 connectTimeout  = 5
 queryTimeout    = 30
 username        = "sample-user"
 password        = "password"
 clusterEndpoint = "sample-cluster.node.us-east-1.docdb.amazonaws.com:27017"

 // Which instances to read from
 readPreference = "secondaryPreferred"

 connectionStringTemplate = "mongodb://%s:%s@%s/sample-database?
tls=true&replicaSet=rs0&readpreference=%s"
)

func main() {

 connectionURI := fmt.Sprintf(connectionStringTemplate, username, password,
 clusterEndpoint, readPreference)

 tlsConfig, err := getCustomTLSConfig(caFilePath)
 if err != nil {
  log.Fatalf("Failed getting TLS configuration: %v", err)
 }

 client, err :=
 mongo.NewClient(options.Client().ApplyURI(connectionURI).SetTLSConfig(tlsConfig))
 if err != nil {
  log.Fatalf("Failed to create client: %v", err)
 }

 ctx, cancel := context.WithTimeout(context.Background(),
 connectTimeout*time.Second)
 defer cancel()
```

```
err = client.Connect(ctx)
if err != nil {
 log.Fatalf("Failed to connect to cluster: %v", err)
}

// Force a connection to verify our connection string
err = client.Ping(ctx, nil)
if err != nil {
 log.Fatalf("Failed to ping cluster: %v", err)
}

fmt.Println("Connected to DocumentDB!")

collection := client.Database("sample-database").Collection("sample-collection")

ctx, cancel = context.WithTimeout(context.Background(), queryTimeout*time.Second)
defer cancel()

res, err := collection.InsertOne(ctx, bson.M{"name": "pi", "value": 3.14159})
if err != nil {
 log.Fatalf("Failed to insert document: %v", err)
}

id := res.InsertedID
log.Printf("Inserted document ID: %s", id)

ctx, cancel = context.WithTimeout(context.Background(), queryTimeout*time.Second)
defer cancel()

cur, err := collection.Find(ctx, bson.D{})

if err != nil {
 log.Fatalf("Failed to run find query: %v", err)
}
defer cur.Close(ctx)

for cur.Next(ctx) {
 var result bson.M
 err := cur.Decode(&result)
 log.Printf("Returned: %v", result)

 if err != nil {
  log.Fatal(err)
```

```
  }
 }

 if err := cur.Err(); err != nil {
  log.Fatal(err)
 }

}

func getCustomTLSConfig(caFile string) (*tls.Config, error) {
 tlsConfig := new(tls.Config)
 certs, err := ioutil.ReadFile(caFile)

 if err != nil {
  return tlsConfig, err
 }

 tlsConfig.RootCAs = x509.NewCertPool()
 ok := tlsConfig.RootCAs.AppendCertsFromPEM(certs)

 if !ok {
  return tlsConfig, errors.New("Failed parsing pem file")
 }

 return tlsConfig, nil
```

Java

Si se conecta a un clúster de Amazon DocumentDB con TLS habilitado desde una aplicación Java, el programa debe utilizar el archivo de la entidad de certificación (CA) proporcionado por AWS para validar la conexión. Para utilizar el certificado de CA de Amazon RDS, haga lo siguiente:

1. Descargue el archivo de CA de Amazon RDS desde https://truststore.pki.rds.amazonaws.com/global/global-bundle.pem .
2. Cree un almacén de confianza con el certificado de CA contenido en el archivo utilizando los siguientes comandos. Asegúrese de cambiar *`truststore-password`* por otra cosa. Si tiene acceso a un almacén de confianza que contiene el certificado de CA antiguo (`rds-ca-2015-root.pem`) y el nuevo certificado de CA (`rds-ca-2019-root.pem`), puede importar el grupo de certificados en el almacén de confianza.

A continuación se muestra un ejemplo de script de shell que importa el paquete de certificados a un almacén de confianza en un sistema operativo Linux. En los ejemplos siguientes, reemplace cada *marcador de posición del usuario* con su propia información. En particular, siempre que se encuentre el directorio de ejemplo "*mydir*" en el script, sustitúyalo por un directorio que haya creado para esta tarea.

```
mydir=/tmp/certs
truststore=${mydir}/rds-truststore.jks
storepassword=truststore-password

curl -sS "https://truststore.pki.rds.amazonaws.com/global/global-bundle.pem" >
 ${mydir}/global-bundle.pem
awk 'split_after == 1 {n++;split_after=0} /-----END CERTIFICATE-----/
 {split_after=1}{print > "rds-ca-" n ".pem"}' < ${mydir}/global-bundle.pem

for CERT in rds-ca-*; do
  alias=$(openssl x509 -noout -text -in $CERT | perl -ne 'next unless /
Subject:/; s/.*(CN=|CN = )//; print')
  echo "Importing $alias"
  keytool -import -file ${CERT} -alias "${alias}" -storepass ${storepassword} -
keystore ${truststore} -noprompt
  rm $CERT
done

rm ${mydir}/global-bundle.pem

echo "Trust store content is: "

keytool -list -v -keystore "$truststore" -storepass ${storepassword} | grep
 Alias | cut -d " " -f3- | while read alias
do
   expiry=`keytool -list -v -keystore "$truststore" -storepass ${storepassword}
 -alias "${alias}" | grep Valid | perl -ne 'if(/until: (.*?)\n/) { print
 "$1\n"; }'`
   echo " Certificate ${alias} expires in '$expiry'"
done
```

A continuación se muestra un ejemplo de script de shell que importa el paquete de certificados a un almacén de confianza en macOS.

```
mydir=/tmp/certs
truststore=${mydir}/rds-truststore.jks
storepassword=truststore-password

curl -sS "https://truststore.pki.rds.amazonaws.com/global/global-bundle.pem" >
 ${mydir}/global-bundle.pem
split -p "-----BEGIN CERTIFICATE-----" ${mydir}/global-bundle.pem rds-ca-

for CERT in rds-ca-*; do
  alias=$(openssl x509 -noout -text -in $CERT | perl -ne 'next unless /
Subject:/; s/.*(CN=|CN = )//; print')
  echo "Importing $alias"
  keytool -import -file ${CERT} -alias "${alias}" -storepass ${storepassword} -
keystore ${truststore} -noprompt
  rm $CERT
done

rm ${mydir}/global-bundle.pem

echo "Trust store content is: "

keytool -list -v -keystore "$truststore" -storepass ${storepassword} | grep
 Alias | cut -d " " -f3- | while read alias
do
   expiry=`keytool -list -v -keystore "$truststore" -storepass ${storepassword}
 -alias "${alias}" | grep Valid | perl -ne 'if(/until: (.*?)\n/) { print
 "$1\n"; }'`
   echo " Certificate ${alias} expires in '$expiry'"
done
```

3. Utilice el `keystore` de su programa estableciendo las siguientes propiedades del sistema en la aplicación antes de establecer una conexión con el clúster de Amazon DocumentDB.

```
javax.net.ssl.trustStore: truststore
javax.net.ssl.trustStorePassword: truststore-password;
```

4. El código siguiente demuestra cómo conectarse a Amazon DocumentDB utilizando Java cuando TLS está habilitado.

   En el siguiente ejemplo, reemplace cada *`marcador de posición del usuario`* con la información de su clúster.

```
package com.example.documentdb;

import com.mongodb.client.*;
import org.bson.Document;

public final class Test {
    private Test() {
    }
    public static void main(String[] args) {

        String template = "mongodb://%s:%s@%s/sample-database?
ssl=true&replicaSet=rs0&readpreference=%s";
        String username = "sample-user";
        String password = "password";
        String clusterEndpoint = "sample-cluster.node.us-
east-1.docdb.amazonaws.com:27017";
        String readPreference = "secondaryPreferred";
        String connectionString = String.format(template, username, password,
 clusterEndpoint, readPreference);

        String truststore = "truststore";
        String truststorePassword = "truststore-password";

        System.setProperty("javax.net.ssl.trustStore", truststore);
        System.setProperty("javax.net.ssl.trustStorePassword",
 truststorePassword);

        MongoClient mongoClient = MongoClients.create(connectionString);

        MongoDatabase testDB = mongoClient.getDatabase("sample-database");
        MongoCollection<Document> numbersCollection =
 testDB.getCollection("sample-collection");

        Document doc = new Document("name", "pi").append("value", 3.14159);
        numbersCollection.insertOne(doc);

        MongoCursor<Document> cursor = numbersCollection.find().iterator();
        try {
            while (cursor.hasNext()) {
                System.out.println(cursor.next().toJson());
            }
        } finally {
            cursor.close();
```

```
        }

    }
}
```

C# / .NET

El código siguiente demuestra cómo conectarse a Amazon DocumentDB utilizando C# / .NET cuando TLS está habilitado.

En el siguiente ejemplo, reemplace cada *marcador de posición del usuario* con la información de su clúster.

```
using System;
using System.Text;
using System.Linq;
using System.Collections.Generic;
using System.Security.Cryptography;
using System.Security.Cryptography.X509Certificates;
using System.Net.Security;
using MongoDB.Driver;
using MongoDB.Bson;

namespace DocDB
{
    class Program
    {
        static void Main(string[] args)
        {
            string template = "mongodb://{0}:{1}@{2}/sampledatabase?
tls=true&replicaSet=rs0&readpreference={3}";
            string username = "sample-user";
            string password = "password";
            string readPreference = "secondaryPreferred";
            string clusterEndpoint="sample-cluster.node.us-
east-1.docdb.amazonaws.com:27017";
            string connectionString = String.Format(template, username, password,
 clusterEndpoint, readPreference);

            string pathToCAFile = "<PATH/global-bundle.p7b_file>";

            // ADD CA certificate to local trust store
```

```
            // DO this once - Maybe when your service starts
            X509Store localTrustStore = new X509Store(StoreName.Root);
            X509Certificate2Collection certificateCollection = new
 X509Certificate2Collection();
            certificateCollection.Import(pathToCAFile);
            try
            {
                localTrustStore.Open(OpenFlags.ReadWrite);
                localTrustStore.AddRange(certificateCollection);
            }
            catch (Exception ex)
            {
                Console.WriteLine("Root certificate import failed: " + ex.Message);
                throw;
            }
            finally
            {
                localTrustStore.Close();
            }

            var settings = MongoClientSettings.FromUrl(new
 MongoUrl(connectionString));
            var client = new MongoClient(settings);

            var database = client.GetDatabase("sampledatabase");
            var collection =
 database.GetCollection<BsonDocument>("samplecollection");
            var docToInsert = new BsonDocument { { "pi", 3.14159 } };
            collection.InsertOne(docToInsert);
        }
    }
}
```

MongoDB Shell

El siguiente código demuestra cómo conectarse a Amazon DocumentDB y realizar consultas mediante la versión más reciente, mongosh, o la versión anterior del shell de mongo cuando TLS está habilitado.

Conexión con Amazon DocumentDB con mongosh

> **Important**
>
> Existe una limitación conocida con los controladores de Node.js anteriores a la versión 6.13.1, ya que Amazon DocumentDB no los admite actualmente para la autenticación de identidad de IAM. Los controladores y las herramientas de Node.js que utilizan el controlador Node.js (por ejemplo, mongosh) deben actualizarse para utilizar el controlador Node.js, versión 6.13.1 o posterior.

En los siguientes ejemplos, reemplace cada *marcador de posición del usuario* con la información de su clúster.

```
mongosh --tls --host cluster-end-point:27017 --tlsCAFile  global-bundle.pem --
username sample-user --password password --retryWrites false
```

Conexión con Amazon DocumentDB con la versión anterior del shell de mongo

Si usa IAM, debe usar una versión anterior del shell de mongo. Introduzca una de las siguientes opciones de comando:

```
mongo --ssl --host cluster-end-point:27017 --sslCAFile global-bundle.pem --
username sample-user --password password
```

Si utiliza una versión igual o superior a la 4.2, utilice el siguiente código para conectarse. Amazon DocumentDB no admite el reintento de las escrituras. Si utiliza el shell de mongo heredado (no mongosh), no incluya el comando `retryWrites=false` en ninguna cadena de código. El reintento de las escrituras está desactivado de forma predeterminada. Incluir `retryWrites=false` podría provocar un error en comandos de lectura normales.

```
mongo --tls --host cluster-end-point:27017 --tlsCAFile global-bundle.pem --
username sample-user --password password
```

Pruebe la conexión

1. Insertar un documento.

   ```
   db.myTestCollection.insertOne({'hello':'Amazon DocumentDB'})
   ```

2. Busque el documento que ha insertado anteriormente.

```
db.myTestCollection.find({'hello':'Amazon DocumentDB'})
```

R

En el siguiente código, se muestra cómo conectarse a Amazon DocumentDB con R usando mongolite (https://jeroen.github.io/mongolite/) cuando TLS está habilitado.

En el siguiente ejemplo, reemplace cada *marcador de posición del usuario* con la información de su clúster.

```
#Include the mongolite library.
library(mongolite)

mongourl <- paste("mongodb://sample-user:password@sample-cluster.node.us-
east-1.docdb.amazonaws.com:27017/test2?ssl=true&",
          "readPreference=secondaryPreferred&replicaSet=rs0", sep="")

#Create a MongoDB client, open a connection to Amazon DocumentDB as a replica
#   set and specify the read preference as secondary preferred
client <-  mongo(url = mongourl, options = ssl_options(weak_cert_validation = F, ca
 ="<PATH/global-bundle.pem>"))

#Insert a single document
str <- c('{"hello" : "Amazon DocumentDB"}')
client$insert(str)

#Find the document that was previously written
client$find()
```

Ruby

El código siguiente demuestra cómo conectarse a Amazon DocumentDB con Ruby cuando TLS está habilitado.

En el siguiente ejemplo, reemplace cada *marcador de posición del usuario* con la información de su clúster.

```
require 'mongo'
require 'neatjson'
require 'json'
client_host = 'mongodb://sample-cluster.node.us-east-1.docdb.amazonaws.com:27017'
```

```
client_options = {
   database: 'test',
   replica_set: 'rs0',
   read: {:secondary_preferred => 1},
   user: 'sample-user',
   password: 'password',
   ssl: true,
   ssl_verify: true,
   ssl_ca_cert: 'PATH/global-bundle.pem',
   retry_writes: false
}


begin
   ##Create a MongoDB client, open a connection to Amazon DocumentDB as a
   ##   replica set and specify the read preference as secondary preferred
   client = Mongo::Client.new(client_host, client_options)

   ##Insert a single document
   x = client[:test].insert_one({"hello":"Amazon DocumentDB"})

   ##Find the document that was previously written
   result = client[:test].find()

   #Print the document
   result.each do |document|
      puts JSON.neat_generate(document)
   end
end

#Close the connection
client.close
```

Conexión con TLS deshabilitado

Para ver un ejemplo de código para conectarse mediante programación a un clúster de Amazon DocumentDB con TLS deshabilitado, elija la pestaña del lenguaje que desea utilizar.

Python

El código siguiente demuestra cómo conectarse a Amazon DocumentDB utilizando Python cuando TLS está deshabilitado.

En el siguiente ejemplo, reemplace cada *marcador de posición del usuario* con la información de su clúster.

```
## Create a MongoDB client, open a connection to Amazon DocumentDB as a replica set
 and specify the read preference as secondary preferred

import pymongo
import sys

client = pymongo.MongoClient('mongodb://sample-user:password@sample-cluster.node.us-
east-1.docdb.amazonaws.com:27017/?
replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')

##Specify the database to be used
db = client.sample_database

##Specify the collection to be used
col = db.sample_collection

##Insert a single document
col.insert_one({'hello':'Amazon DocumentDB'})

##Find the document that was previously written
x = col.find_one({'hello':'Amazon DocumentDB'})

##Print the result to the screen
print(x)

##Close the connection
client.close()
```

Node.js

El código siguiente demuestra cómo conectarse a Amazon DocumentDB utilizando Node.js cuando TLS está deshabilitado.

> **Important**
>
> Existe una limitación conocida con los controladores de Node.js anteriores a la versión 6.13.1, ya que Amazon DocumentDB no los admite actualmente para la autenticación de identidad de IAM. Los controladores y las herramientas de Node.js que

utilizan el controlador Node.js (por ejemplo, mongosh) deben actualizarse para utilizar el controlador Node.js, versión 6.13.1 o posterior.

En el siguiente ejemplo, reemplace cada *marcador de posición del usuario* con la información de su clúster.

```
var MongoClient = require('mongodb').MongoClient;

//Create a MongoDB client, open a connection to Amazon DocumentDB as a replica set,
//  and specify the read preference as secondary preferred
var client = MongoClient.connect(
'mongodb://sample-user:password@sample-cluster.node.us-
east-1.docdb.amazonaws.com:27017/sample-database?
replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false',
{
  useNewUrlParser: true
},

function(err, client) {
    if(err)
        throw err;
    //Specify the database to be used
    db = client.db('sample-database');

    //Specify the collection to be used
    col = db.collection('sample-collection');

    //Insert a single document
    col.insertOne({'hello':'Amazon DocumentDB'}, function(err, result){
      //Find the document that was previously written
      col.findOne({'hello':'Amazon DocumentDB'}, function(err, result){
        //Print the result to the screen
        console.log(result);

        //Close the connection
        client.close()
      });
   });
});
```

PHP

El código siguiente demuestra cómo conectarse a Amazon DocumentDB utilizando PHP cuando TLS está deshabilitado.

En el siguiente ejemplo, reemplace cada *marcador de posición del usuario* con la información de su clúster.

```
<?php
//Include Composer's autoloader
require 'vendor/autoload.php';

//Create a MongoDB client and open connection to Amazon DocumentDB
$client = new MongoDB\Client("mongodb://sample-user:password@sample-cluster.node.us-
east-1.docdb.amazonaws.com:27017/?retryWrites=false");

//Specify the database and collection to be used
$col = $client->sampledatabase->samplecollection;

//Insert a single document
$result = $col->insertOne( [ 'hello' => 'Amazon DocumentDB'] );

//Find the document that was previously written
$result = $col->findOne(array('hello' => 'Amazon DocumentDB'));

//Print the result to the screen
print_r($result);
?>
```

Go

El código siguiente demuestra cómo conectarse a Amazon DocumentDB utilizando Go cuando TLS está deshabilitado.

En el siguiente ejemplo, reemplace cada *marcador de posición del usuario* con la información de su clúster.

```
package main

import (
 "context"
 "fmt"
 "log"
```

```
 "time"

 "go.mongodb.org/mongo-driver/bson"
 "go.mongodb.org/mongo-driver/mongo"
 "go.mongodb.org/mongo-driver/mongo/options"
)

const (
 // Timeout operations after N seconds
 connectTimeout  = 5
 queryTimeout    = 30
 username        = "sample-user"
 password        = "password"
 clusterEndpoint = "sample-cluster.node.us-east-1.docdb.amazonaws.com:27017"

 // Which instances to read from
 readPreference           = "secondaryPreferred"
 connectionStringTemplate = "mongodb://%s:%s@%s/sample-database?
replicaSet=rs0&readpreference=%s"
)

func main() {

 connectionURI := fmt.Sprintf(connectionStringTemplate, username, password,
 clusterEndpoint, readPreference)

 client, err := mongo.NewClient(options.Client().ApplyURI(connectionURI))
 if err != nil {
  log.Fatalf("Failed to create client: %v", err)
 }

 ctx, cancel := context.WithTimeout(context.Background(),
 connectTimeout*time.Second)
 defer cancel()

 err = client.Connect(ctx)
 if err != nil {
  log.Fatalf("Failed to connect to cluster: %v", err)
 }

 // Force a connection to verify our connection string
 err = client.Ping(ctx, nil)
 if err != nil {
  log.Fatalf("Failed to ping cluster: %v", err)
```

```
 }

 fmt.Println("Connected to DocumentDB!")

 collection := client.Database("sample-database").Collection("sample-collection")

 ctx, cancel = context.WithTimeout(context.Background(), queryTimeout*time.Second)
 defer cancel()

 res, err := collection.InsertOne(ctx, bson.M{"name": "pi", "value": 3.14159})
 if err != nil {
  log.Fatalf("Failed to insert document: %v", err)
 }

 id := res.InsertedID
 log.Printf("Inserted document ID: %s", id)

 ctx, cancel = context.WithTimeout(context.Background(), queryTimeout*time.Second)
 defer cancel()

 cur, err := collection.Find(ctx, bson.D{})

 if err != nil {
  log.Fatalf("Failed to run find query: %v", err)
 }
 defer cur.Close(ctx)

 for cur.Next(ctx) {
  var result bson.M
  err := cur.Decode(&result)
  log.Printf("Returned: %v", result)

  if err != nil {
   log.Fatal(err)
  }
 }

 if err := cur.Err(); err != nil {
  log.Fatal(err)
 }

}
```

Java

El código siguiente demuestra cómo conectarse a Amazon DocumentDB utilizando Java cuando TLS está deshabilitado.

En el siguiente ejemplo, reemplace cada *marcador de posición del usuario* con la información de su clúster.

```
package com.example.documentdb;

import com.mongodb.MongoClient;
import com.mongodb.MongoClientURI;
import com.mongodb.ServerAddress;
import com.mongodb.MongoException;
import com.mongodb.client.MongoCursor;
import com.mongodb.client.MongoDatabase;
import com.mongodb.client.MongoCollection;
import org.bson.Document;


public final class Main {
    private Main() {
    }
    public static void main(String[] args) {

        String template = "mongodb://%s:%s@%s/sample-database?
replicaSet=rs0&readpreference=%s";
        String username = "sample-user";
        String password = "password";
        String clusterEndpoint = "sample-cluster.node.us-
east-1.docdb.amazonaws.com:27017";
        String readPreference = "secondaryPreferred";
        String connectionString = String.format(template, username, password,
 clusterEndpoint, readPreference);

        MongoClientURI clientURI = new MongoClientURI(connectionString);
        MongoClient mongoClient = new MongoClient(clientURI);

        MongoDatabase testDB = mongoClient.getDatabase("sample-database");
        MongoCollection<Document> numbersCollection = testDB.getCollection("sample-
collection");

        Document doc = new Document("name", "pi").append("value", 3.14159);
```

```
        numbersCollection.insertOne(doc);

        MongoCursor<Document> cursor = numbersCollection.find().iterator();
        try {
            while (cursor.hasNext()) {
                System.out.println(cursor.next().toJson());
            }
        } finally {
            cursor.close();
        }

    }
}
```

C# / .NET

El código siguiente demuestra cómo conectarse a Amazon DocumentDB utilizando C# / .NET cuando TLS está deshabilitado.

En el siguiente ejemplo, reemplace cada *marcador de posición del usuario* con la información de su clúster.

```
using System;
using System.Text;
using System.Linq;
using System.Collections.Generic;
using System.Security.Cryptography;
using System.Security.Cryptography.X509Certificates;
using System.Net.Security;
using MongoDB.Driver;
using MongoDB.Bson;

namespace CSharpSample
{
   class Program
    {
       static void Main(string[] args)
        {
           string template = "mongodb://{0}:{1}@{2}/sampledatabase?
replicaSet=rs0&readpreference={3}";
           string username = "sample-user";
           string password = "password";
```

```
            string clusterEndpoint = "sample-cluster.node.us-
east-1.docdb.amazonaws.com:27017";
            string readPreference = "secondaryPreferred";
            string connectionString = String.Format(template, username, password,
 clusterEndpoint, readPreference);

            var settings = MongoClientSettings.FromUrl(new
 MongoUrl(connectionString));
            var client = new MongoClient(settings);

            var database = client.GetDatabase("sampledatabase");
            var collection =
 database.GetCollection<BsonDocument>("samplecollection");
            var docToInsert = new BsonDocument { { "pi", 3.14159 } };
             collection.InsertOne(docToInsert);
        }
    }
}
```

MongoDB Shell

El siguiente código demuestra cómo conectarse a Amazon DocumentDB y realizar consultas mediante la versión más reciente, mongosh, o la versión anterior del shell de mongo cuando TLS está deshabilitado.

Conexión con Amazon DocumentDB con mongosh

> **Important**
>
> Existe una limitación conocida con los controladores de Node.js anteriores a la versión 6.13.1, ya que Amazon DocumentDB no los admite actualmente para la autenticación de identidad de IAM. Los controladores y las herramientas de Node.js que utilizan el controlador Node.js (por ejemplo, mongosh) deben actualizarse para utilizar el controlador Node.js, versión 6.13.1 o posterior.

En los siguientes ejemplos, reemplace cada *marcador de posición del usuario* con la información de su clúster.

```
mongosh --host cluster-end-point:27017 --username sample-user --password password --
retryWrites false
```

Conexión con Amazon DocumentDB con la versión anterior del shell de mongo

Si usa IAM, debe usar una versión anterior del shell de mongo. Introduzca una de las siguientes opciones de comando:

```
mongo --host cluster-end-point:27017 --username sample-user --password password
```

Si utiliza una versión igual o superior a la 4.2, utilice el siguiente código para conectarse. Amazon DocumentDB no admite el reintento de las escrituras. Si utiliza el shell de mongo heredado (no mongosh), no incluya el comando `retryWrites=false` en ninguna cadena de código. El reintento de las escrituras está desactivado de forma predeterminada. Incluir `retryWrites=false` podría provocar un error en comandos de lectura normales.

```
mongo --host cluster-end-point:27017 --username sample-user --password password
```

Pruebe la conexión

1. Insertar un documento.

   ```
   db.myTestCollection.insertOne({'hello':'Amazon DocumentDB'})
   ```

2. Busque el documento que ha insertado anteriormente.

   ```
   db.myTestCollection.find({'hello':'Amazon DocumentDB'})
   ```

R

En el siguiente código, se muestra cómo conectarse a Amazon DocumentDB con R usando mongolite (https://jeroen.github.io/mongolite/) cuando TLS está deshabilitado.

En el siguiente ejemplo, reemplace cada *marcador de posición del usuario* con la información de su clúster.

```
#Include the mongolite library.
library(mongolite)

#Create a MongoDB client, open a connection to Amazon DocumentDB as a replica
#   set and specify the read preference as secondary preferred
```

```
client <- mongo(url = "mongodb://sample-user:password@sample-
cluster.node.us-east-1.docdb.amazonaws.com:27017/sample-database?
readPreference=secondaryPreferred&replicaSet=rs0")

##Insert a single document
str <- c('{"hello" : "Amazon DocumentDB"}')
client$insert(str)

##Find the document that was previously written
client$find()
```

Ruby

El código siguiente demuestra cómo conectarse a Amazon DocumentDB con Ruby cuando TLS está deshabilitado.

En el siguiente ejemplo, reemplace cada *marcador de posición del usuario* con la información de su clúster.

```
require 'mongo'
require 'neatjson'
require 'json'
client_host = 'mongodb://sample-cluster.node.us-east-1.docdb.amazonaws.com:27017'
client_options = {
   database: 'test',
   replica_set: 'rs0',
   read: {:secondary_preferred => 1},
   user: 'sample-user',
   password: 'password',
   retry_writes: false
}

begin
   ##Create a MongoDB client, open a connection to Amazon DocumentDB as a
   ##   replica set and specify the read preference as secondary preferred
   client = Mongo::Client.new(client_host, client_options)

   ##Insert a single document
   x = client[:test].insert_one({"hello":"Amazon DocumentDB"})

   ##Find the document that was previously written
   result = client[:test].find()
```

```
   #Print the document
   result.each do |document|
      puts JSON.neat_generate(document)
   end
end

#Close the connection
client.close
```

Conexión a un clúster de Amazon DocumentDB desde fuera de una Amazon VPC

Los clústeres de Amazon DocumentDB (con compatibilidad con MongoDB) se implementan en una instancia de Amazon Virtual Private Cloud (Amazon VPC). Se puede obtener acceso a ellos directamente mediante instancias de Amazon EC2 u otros servicios de AWS que se implementen en la misma Amazon VPC. Además, es posible obtener acceso a Amazon DocumentDB mediante instancias EC2 u otros servicios de AWS en diferentes VPC de la misma región de Región de AWS u otras regiones a través de la interconexión de VPC.

Sin embargo, supongamos que su caso de uso requiere que usted o su aplicación tengan acceso a los recursos de Amazon DocumentDB desde fuera de la VPC del clúster. En ese caso, puede utilizar la tunelización SSH (denominada también reenvío de puertos) para obtener acceso a sus recursos de Amazon DocumentDB.

La descripción detallada de la tunelización SSH queda fuera del alcance de este tema. Si desea obtener más información sobre la tunelización SSH, consulte los siguientes temas:

- Túnel SSH
- SSH Port Forwarding Example, en concreto la sección Local Forwarding

Para crear un túnel SSH, necesita una instancia de Amazon EC2 que se ejecute en la misma VPC de Amazon que el clúster de Amazon DocumentDB. Puede usar una instancia EC2 existente en la misma VPC que el clúster o crear una. Para obtener más información, consulte el tema correspondiente a su sistema operativo:

- Introducción a las instancias Linux de Amazon EC2
- Introducción a las instancias de Windows de Amazon EC2

Es posible que normalmente se conecte a una instancia EC2 con el siguiente comando:

```
ssh -i "ec2Access.pem" ubuntu@ec2-34-229-221-164.compute-1.amazonaws.com
```

Si es así, puede configurar un túnel de SSH en el clúster de Amazon DocumentDB `sample-cluster.node.us-east-1.docdb.amazonaws.com` ejecutando el siguiente comando en el equipo local. La marca `-L` se utiliza para el reenvío de un puerto local. Cuando utilice un túnel SSH, es recomendable que se conecte al clúster utilizando el punto de conexión de dicho clúster y que no intente conectarse utilizando el modo de conjunto de réplicas (es decir, especificando `replicaSet=rs0` en la cadena de conexión), ya que dará lugar a un error.

```
ssh -i "ec2Access.pem" -L 27017:sample-cluster.node.us-east-1.docdb.amazonaws.com:27017
 ubuntu@ec2-34-229-221-164.compute-1.amazonaws.com -N
```

Una vez creado el túnel SSH, cualquier comando que envíe a `localhost:27017` se reenvía al clúster de Amazon DocumentDB `sample-cluster` que se ejecuta en la VPC de Amazon. Si la seguridad de la capa de transporte (TLS) está habilitada en el clúster de Amazon DocumentDB, tiene que descargar la clave pública de Amazon DocumentDB desde https://truststore.pki.rds.amazonaws.com/global/global-bundle.pem . La siguiente operación descarga este archivo:

```
wget https://truststore.pki.rds.amazonaws.com/global/global-bundle.pem
```

> **Note**
>
> TLS está habilitado de forma predeterminada para los nuevos clústeres de Amazon DocumentDB. No obstante, sí puede deshabilitarlo. Para obtener más información, consulte Administración de la configuración de TLS del clúster de Amazon DocumentDB.

Para conectarse a su clúster de Amazon DocumentDB desde fuera de Amazon VPC, utilice el comando siguiente.

```
mongo --sslAllowInvalidHostnames --ssl --sslCAFile global-bundle.pem --username
 <yourUsername> --password <yourPassword>
```

Conexión a Amazon DocumentDB como conjunto de réplicas

Cuando desarrolle en Amazon DocumentDB (con compatibilidad con MongoDB), recomendamos que se conecte al clúster como conjunto de réplicas y distribuya las lecturas a las instancias de réplica mediante las funciones integradas de preferencias de lectura del controlador. En esta sección se profundiza en lo que esto significa y se describe cómo conectarse al clúster de Amazon DocumentDB como conjunto de réplicas con el SDK para Python como ejemplo.

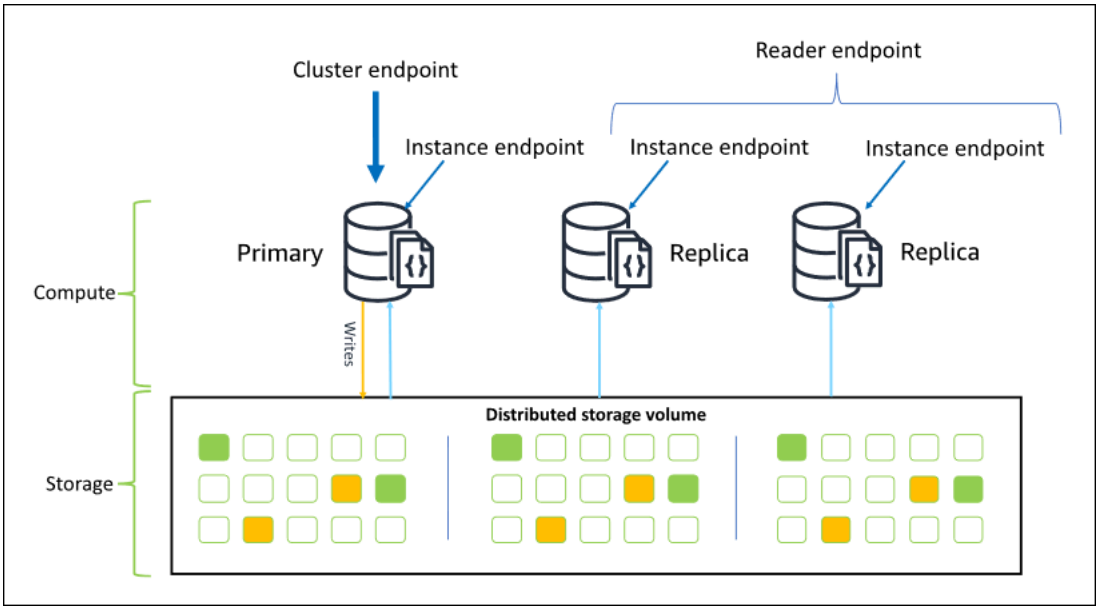
Amazon DocumentDB tiene tres puntos de conexión que puede utilizar para conectarse al clúster:

- Punto de conexión de clúster
- Punto de conexión del lector
- Puntos de conexión de instancia

En la mayoría de los casos, cuando se conecte a Amazon DocumentDB, recomendamos que utilice el punto de conexión de clúster. Se trata de un CNAME que apunta a la instancia principal del clúster, tal y como se muestra en el siguiente diagrama.

Cuando utilice un túnel SSH, es recomendable que se conecte al clúster utilizando el punto de conexión de dicho clúster y que no intente conectarse utilizando el modo de conjunto de réplicas (es decir, especificando `replicaSet=rs0` en la cadena de conexión), ya que dará lugar a un error.

> **Note**
>
> Para obtener más información acerca de los puntos de conexión de sitio web de Amazon DocumentDB, consulte Puntos de conexión de Amazon DocumentDB.



Con el punto de conexión de clúster, puede conectarse al clúster en modo de conjunto de réplicas. A continuación, puede utilizar las funciones integradas del controlador de preferencias de lectura. En el siguiente ejemplo, al especificar `/?replicaSet=rs0`, el SDK entiende que desea conectarse como conjunto de réplicas. Si omite `/?replicaSet=rs0'`, el cliente dirige todas las solicitudes al punto de conexión de clúster, es decir, la instancia principal.

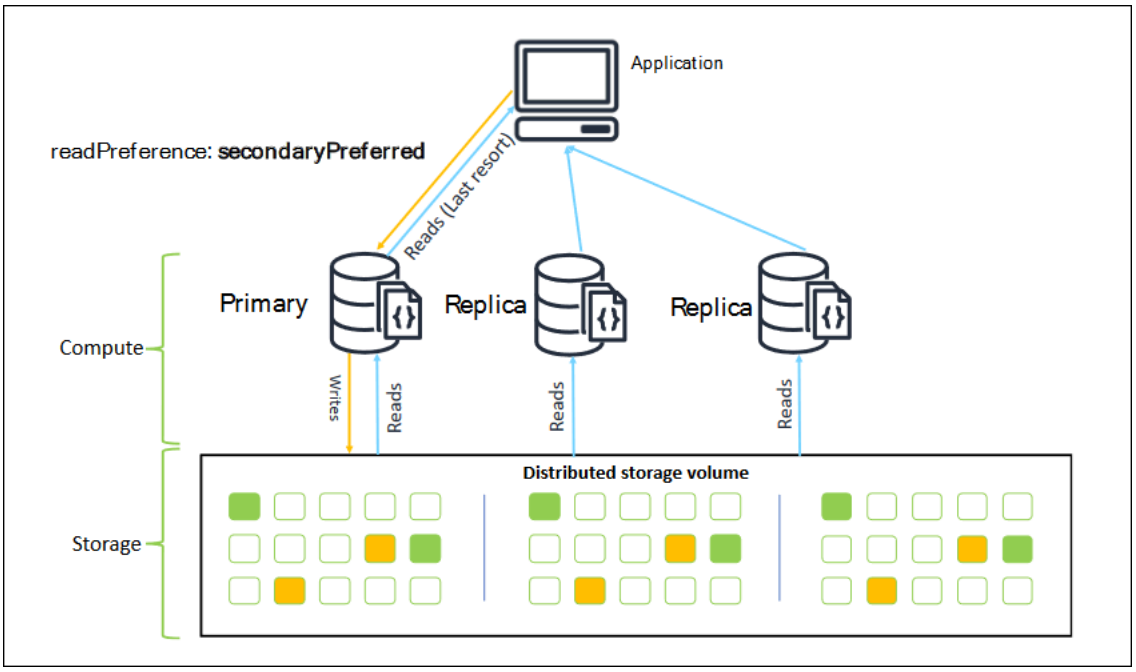
```
## Create a MongoDB client, open a connection to Amazon DocumentDB as a
   ## replica set and specify the read preference as secondary preferred
   client = pymongo.MongoClient('mongodb://<user-name>:<password>@mycluster.node.us-
east-1.docdb.amazonaws.com:27017/?replicaSet=rs0')
```

La ventaja de conectarse como conjunto de réplicas es que permite al SDK detectar automáticamente la topografía del clúster, lo que incluye cuándo se añaden o se eliminan instancias del clúster. Posteriormente, puede utilizar el clúster de forma más eficiente dirigiendo las solicitudes de lectura a las instancias de réplica.

Cuando se conecta como conjunto de réplicas, puede especificar la `readPreference` para la conexión. Si especifica una preferencia de lectura de `secondaryPreferred`, el cliente dirige las consultas de lectura a las réplicas y las consultas de escritura, a la instancia principal (como en el siguiente diagrama). Así, se aprovechan mejor los recursos del clúster. Para obtener más información, consulte Opciones de preferencia de lectura.

```
## Create a MongoDB client, open a connection to Amazon DocumentDB as a
   ##   replica set and specify the read preference as secondary preferred
```

```
client = pymongo.MongoClient('mongodb://<user-name>:<password>@mycluster.node.us-
east-1.docdb.amazonaws.com:27017/?replicaSet=rs0&readPreference=secondaryPreferred')
```



Las lecturas de las réplicas de Amazon DocumentDB presentan consistencia final. Devuelven los datos en el mismo orden en que se escribieron en la instancia principal y, a menudo, hay un retardo de replicación inferior a 50 ms. Puede monitorizar el retardo de réplica del clúster con las métricas de Amazon CloudWatch `DBInstanceReplicaLag` y `DBClusterReplicaLagMaximum`. Para obtener más información, consulte Supervisión de Amazon DocumentDB con CloudWatch.

A diferencia de la arquitectura monolítica tradicional de las bases de datos, Amazon DocumentDB separa el almacenamiento y la computación. Dada esta arquitectura moderna, le animamos a escalar la lectura en las instancias de réplica. Las lecturas en las instancias de réplica no bloquean la replicación de las escrituras desde la instancia principal. Puede añadir hasta 15 instancias de réplica de lectura en un clúster y escalar a millones de lecturas por segundo.

La ventaja principal de conectarse como conjunto de réplicas y distribuir las lecturas a las réplicas es que aumenta los recursos generales del clúster disponibles para utilizar la aplicación. Recomendamos que se conecte como conjunto de réplicas como práctica recomendada. Además, lo recomendamos con más frecuencia en las siguientes situaciones:

- Si utiliza casi el 100 % de la CPU en la instancia principal.
- Si la proporción de aciertos de la caché del búfer es casi cero.
- Si alcanza los límites de conexión o cursor de una instancia.

Escalar el tamaño de una instancia de clúster es una opción y, en algunos casos, puede ser la mejor manera de escalar el clúster. Sin embargo, también deberá plantearse cómo aprovechar mejor las réplicas que ya tiene en el clúster. Esto le permite aumentar la escala sin el mayor coste de utilizar un tipo de instancia mayor. También recomendamos que monitorice y alerte de estos límites (es decir, `CPUUtilization`, `DatabaseConnections` y `BufferCacheHitRatio`) mediante las alarmas de CloudWatch para saber cuándo se está utilizando mucho un recurso.

Para obtener más información, consulte los temas siguientes:

- Prácticas recomendadas para Amazon DocumentDB
- Cuotas y límites de Amazon DocumentDB

Uso de las conexiones del clúster

Plantéese la posibilidad de utilizar todas las conexiones del clúster. Por ejemplo, una instancia `r5.2xlarge` tiene un límite de 4500 conexiones (y 450 cursores abiertos). Si crea un clúster de Amazon DocumentDB de tres instancias y se conecta únicamente a la instancia principal mediante el punto de conexión de clúster, los límites de conexiones y cursores abiertos del clúster son de 4500 y 450 respectivamente. Podría alcanzar estos límites al crear aplicaciones que utilizan muchos procesos de trabajo que se ponen en marcha en contenedores. Los contenedores abren una serie de conexiones a la vez y saturan el clúster.

En su lugar, podría conectarse al clúster de Amazon DocumentDB como conjunto de réplicas y distribuir las lecturas a las instancias de réplica. A continuación, podría triplicar de forma eficaz el número de conexiones y cursores disponibles en el clúster a 13 500 y 1350 respectivamente. Añadir más instancias al clúster solo aumenta el número de conexiones y cursores para las cargas de trabajo de lectura. Si necesita aumentar el número de conexiones para las escrituras en el clúster, recomendamos que aumente el tamaño de la instancia.

> **Note**
>
> El número de conexiones para las instancias `large`, `xlarge` y `2xlarge` aumenta con el tamaño de instancia hasta 4500. El número máximo de conexiones por instancia para instancias `4xlarge` o superiores es 4500. Para obtener más información sobre los límites por tipos de instancia, consulte Límites de instancias.

Normalmente, no recomendamos que se conecte al clúster con la preferencia de lectura de `secondary`. Esto se debe a que, si no hay instancias de réplica en el clúster, las lecturas generarán un error. Por ejemplo, suponga que tiene un clúster de Amazon DocumentDB de dos instancias con una instancia principal y una réplica. Si la réplica tiene un problema, se generará un error en las solicitudes de lectura de un grupo de conexiones establecido como `secondary`. La ventaja de `secondaryPreferred` es que, si el cliente no encuentra una instancia de réplica adecuada a la que conectarse, recurre a la instancia principal para las lecturas.

Varios grupos de conexiones

En algunos casos, las lecturas de una aplicación deben contar con consistencia de lectura tras escritura, que solo se puede distribuir desde la instancia principal en Amazon DocumentDB. En estos casos, podría crear dos grupos de conexiones del cliente: uno para escrituras y otro para lecturas que necesiten consistencia de lectura tras escritura. Para ello, el código tendría un aspecto similar al siguiente.

```
## Create a MongoDB client,
##    open a connection to Amazon DocumentDB as a replica set and specify the
 readPreference as primary
clientPrimary = pymongo.MongoClient('mongodb://<user-
name>:<password>@mycluster.node.us-east-1.docdb.amazonaws.com:27017/?
replicaSet=rs0&readPreference=primary')

## Create a MongoDB client,
##    open a connection to Amazon DocumentDB as a replica set and specify the
 readPreference as secondaryPreferred
secondaryPreferred = pymongo.MongoClient('mongodb://<user-
name>:<password>@mycluster.node.us-east-1.docdb.amazonaws.com:27017/?
replicaSet=rs0&readPreference=secondaryPreferred')
```

Otra opción consiste en crear un único grupo de conexiones y sobrescribir la preferencia de lectura en una colección determinada.

```
##Specify the collection and set the read preference level for that collection
col = db.review.with_options(read_preference=ReadPreference.SECONDARY_PREFERRED)
```

Resumen

Para aprovechar mejor los recursos del clúster, recomendamos que se conecte al clúster mediante el modo de conjunto de réplicas. Si es adecuado para la aplicación, puede escalar la lectura de la aplicación distribuyendo las lecturas a las instancias de réplica.

Conexión a un clúster de Amazon DocumentDB desde Studio 3T

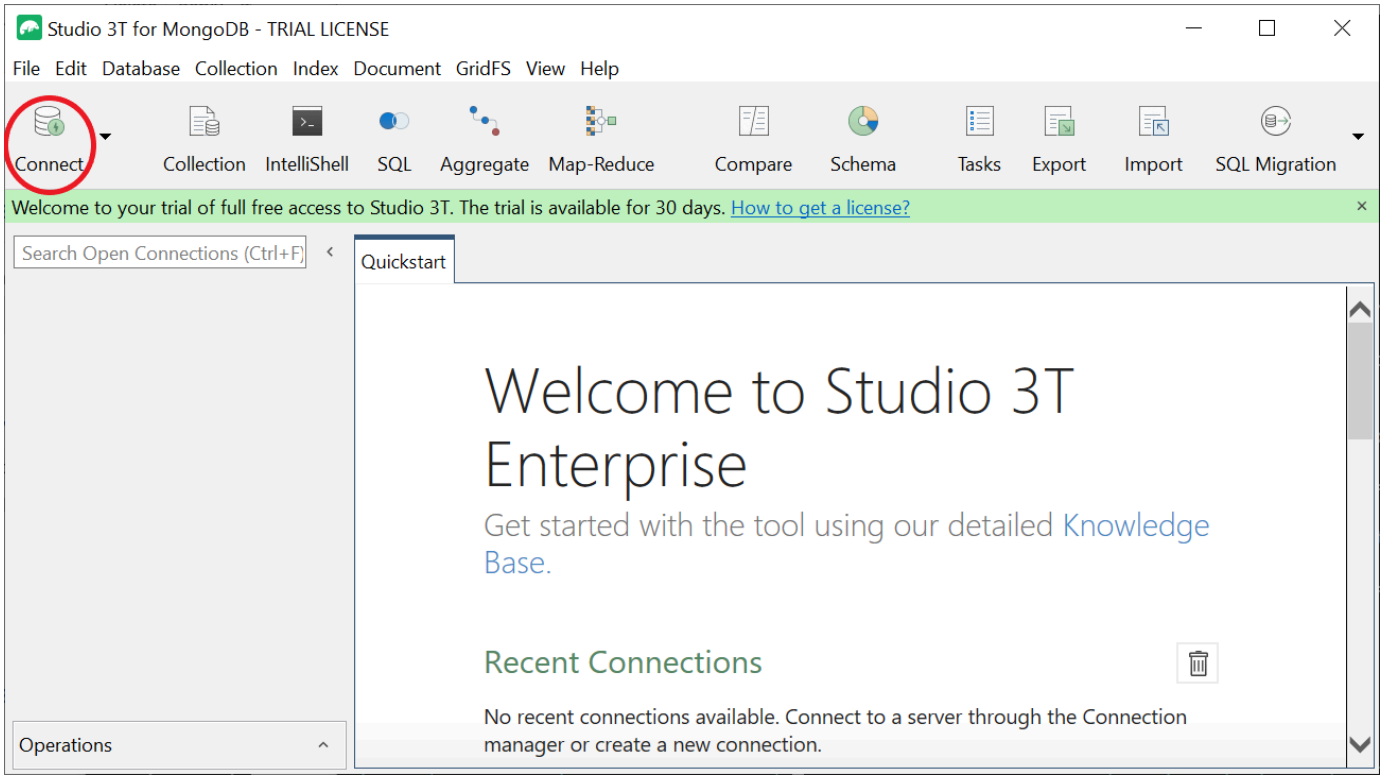
Studio 3T es una GUI e IDE popular para desarrolladores e ingenieros de datos que trabajan con MongoDB. Ofrece varias funciones potentes: vistas de los datos en árbol, tabla y JSON; fácil importación/exportación en CSV, JSON, SQL y BSON/MongoDump; una opción de consulta flexible; una interfaz de usuario visual de arrastrar y soltar; un shell mongo integrado con autocompletado, un editor de canalizaciones de agregación y soporte para consultas SQL.

Requisitos previos

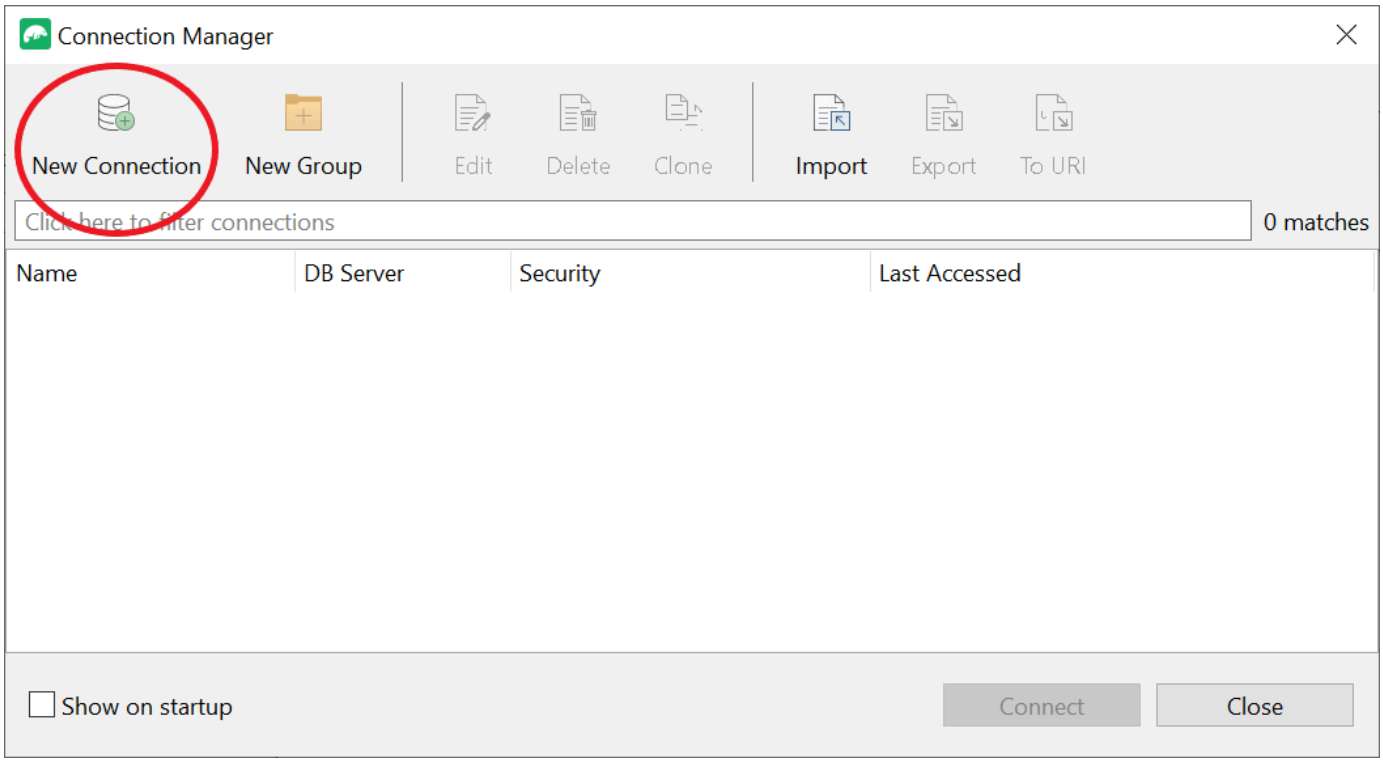
- Si aún no tiene un clúster de Amazon DocumentDB que use Amazon EC2 como bastión o host de salto, siga las instrucciones sobre cómo Conectar con Amazon EC2.
- Si no tiene Studio 3T, descárguelo e instálelo.

Conexión con Studio 3T

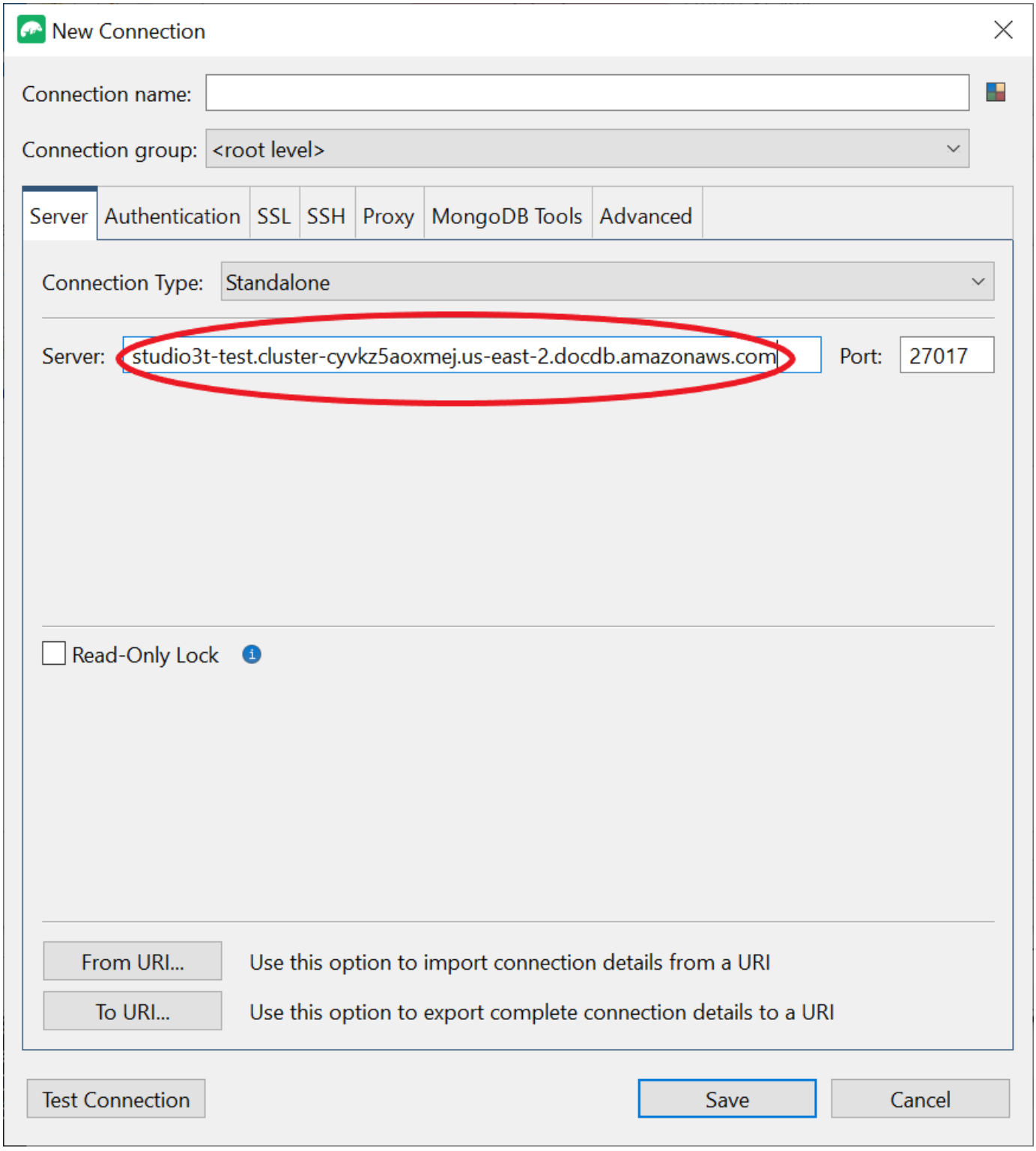
1. Seleccione Conectar en la esquina superior izquierda de la barra de herramientas.



2. Seleccione Nueva conexión en la esquina superior izquierda de la barra de herramientas.

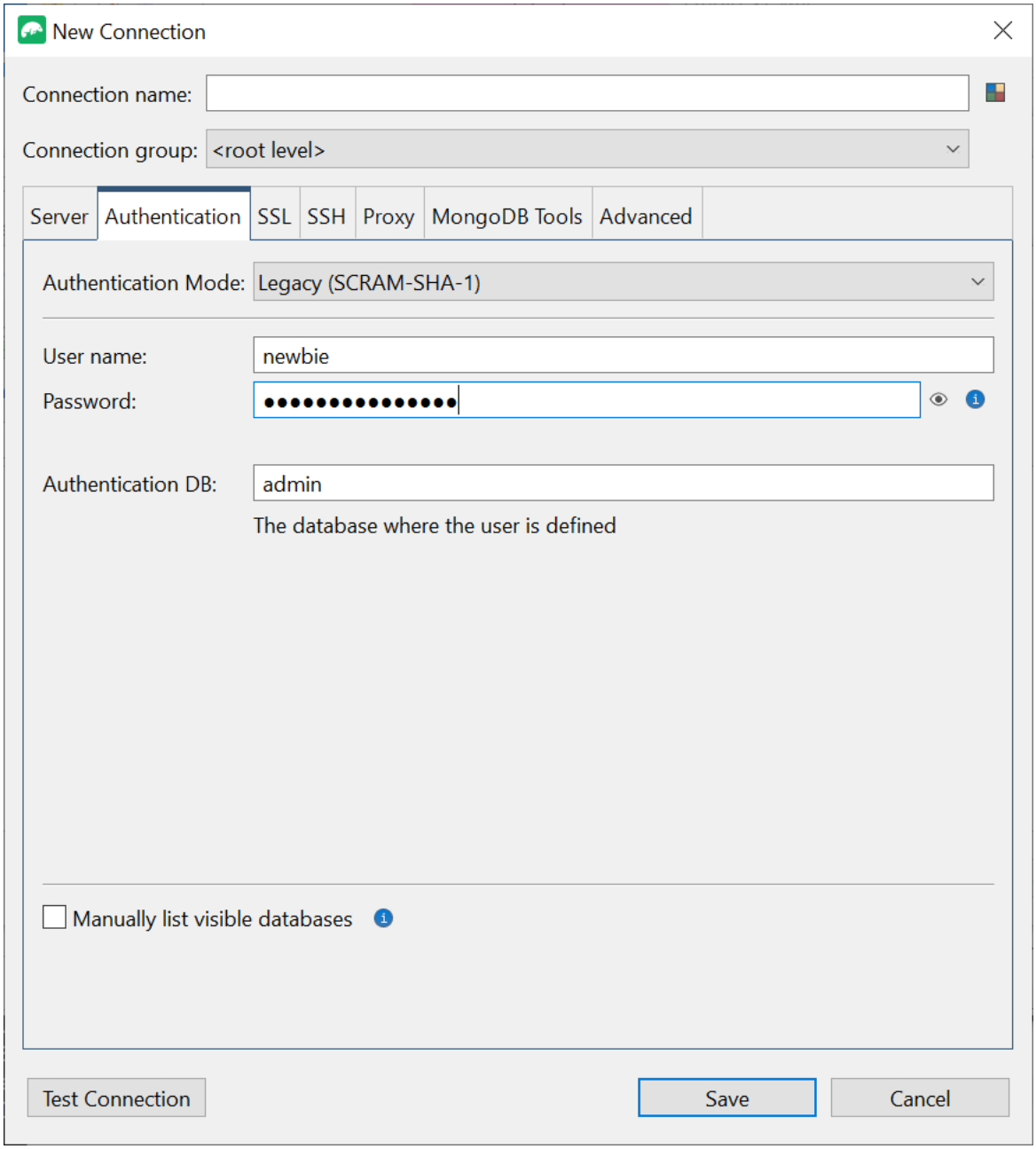


3. En la pestaña Servidor, en el campo Servidor, introduzca la información del punto de conexión del clúster.

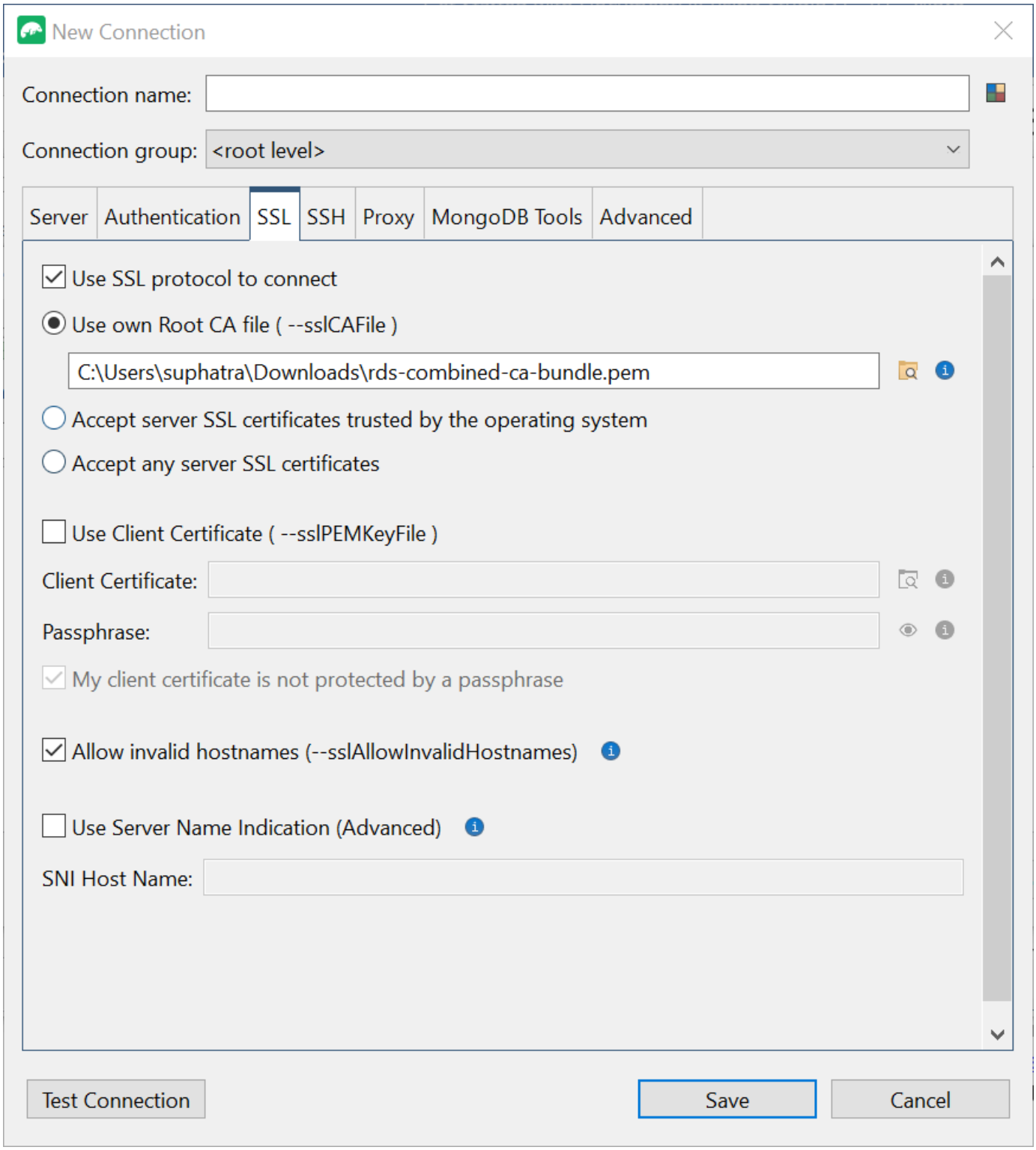

New Connection
Connection name:
Connection group: <root level>
Server
Authentication
SSL
SSH
Proxy
MongoDB Tools
Advanced
Connection Type: Standalone
Server: studio3t-test.cluster-cyvkz5aoxmej.us-east-2.docdb.amazonaws.com
Port: 27017
Read-Only Lock
From URI...
Use this option to import connection details from a URI
To URI...
Use this option to export complete connection details to a URI
Test Connection
Save
Cancel

> **Note**
>
> ¿No encuentra el punto de conexión de su clúster? Solo tiene que seguir los pasos que se indican aquí.

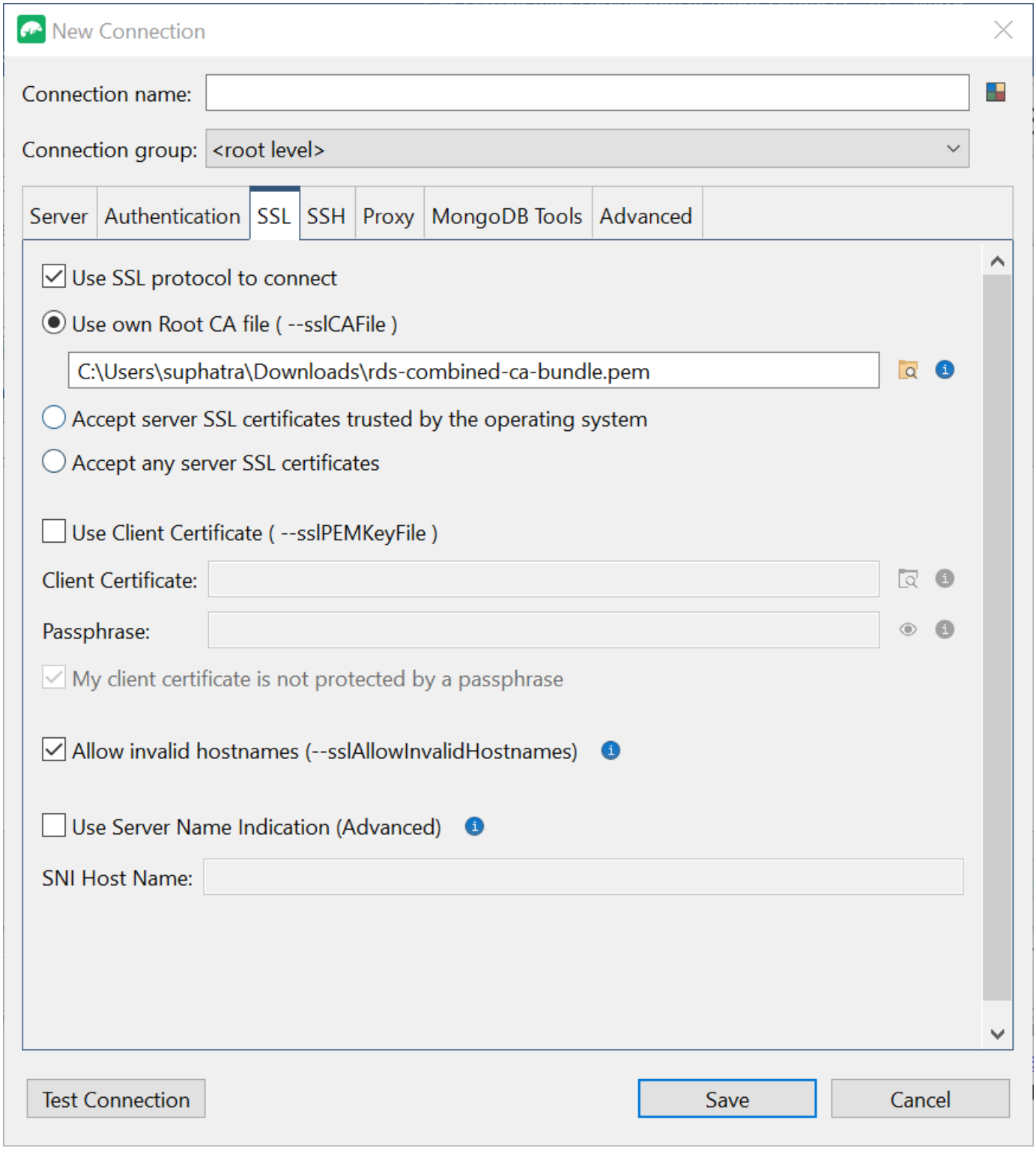
4. Elija la pestaña Autenticación y seleccione Heredado en el menú desplegable Modo de autenticación.



5. Introduzca su nombre de usuario y sus credenciales en los campos Nombre de usuario y Contraseña.
6. Seleccione la pestaña SSL y marque la casilla Usar el protocolo SSL para conectarse.



7. Seleccione Usar un archivo CA raíz propio. A continuación, añada el certificado de Amazon DocumentDB (puede omitir este paso si SSL está deshabilitado en su clúster de DocumentDB). Marque la casilla para permitir nombres de host no válidos.



> **Note**
>
> ¿No tiene el certificado? Puede descargarlo con el siguiente comando:
> `wget https://truststore.pki.rds.amazonaws.com/global/global-bundle.pem`

8. Si se conecta desde una máquina cliente externa a Amazon VPC, debe crear un túnel SSH. Hará esto en la pestaña SSH.

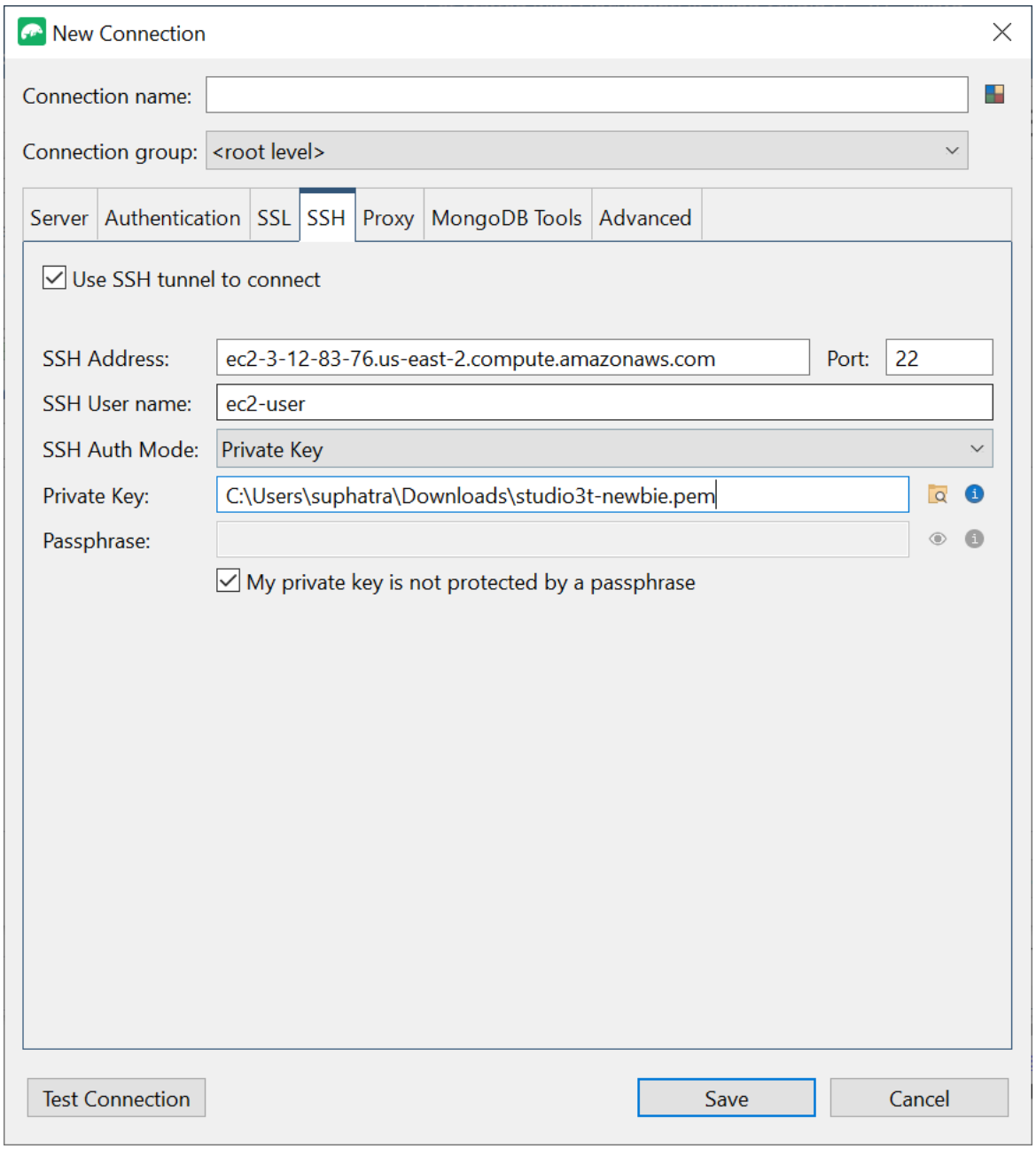
   a. Marque la casilla Usar túnel SSH e introduzca la dirección SSH en el campo Dirección SSH. Este es el DNS público (IPV4) de su instancia. Puede obtener esta URL desde su Consola de administración de Amazon EC2.

   b. Introduzca su nombre de usuario. Este es el nombre de usuario de su instancia de Amazon EC2.

   c. Como Modo de autenticación SSH, seleccione Clave privada. En el campo Clave privada, elija el icono del buscador de archivos para localizar y elegir la clave privada de su instancia de Amazon EC2. Este es el archivo .pem (par de claves) que guardó al crear la instancia en la consola de Amazon EC2.

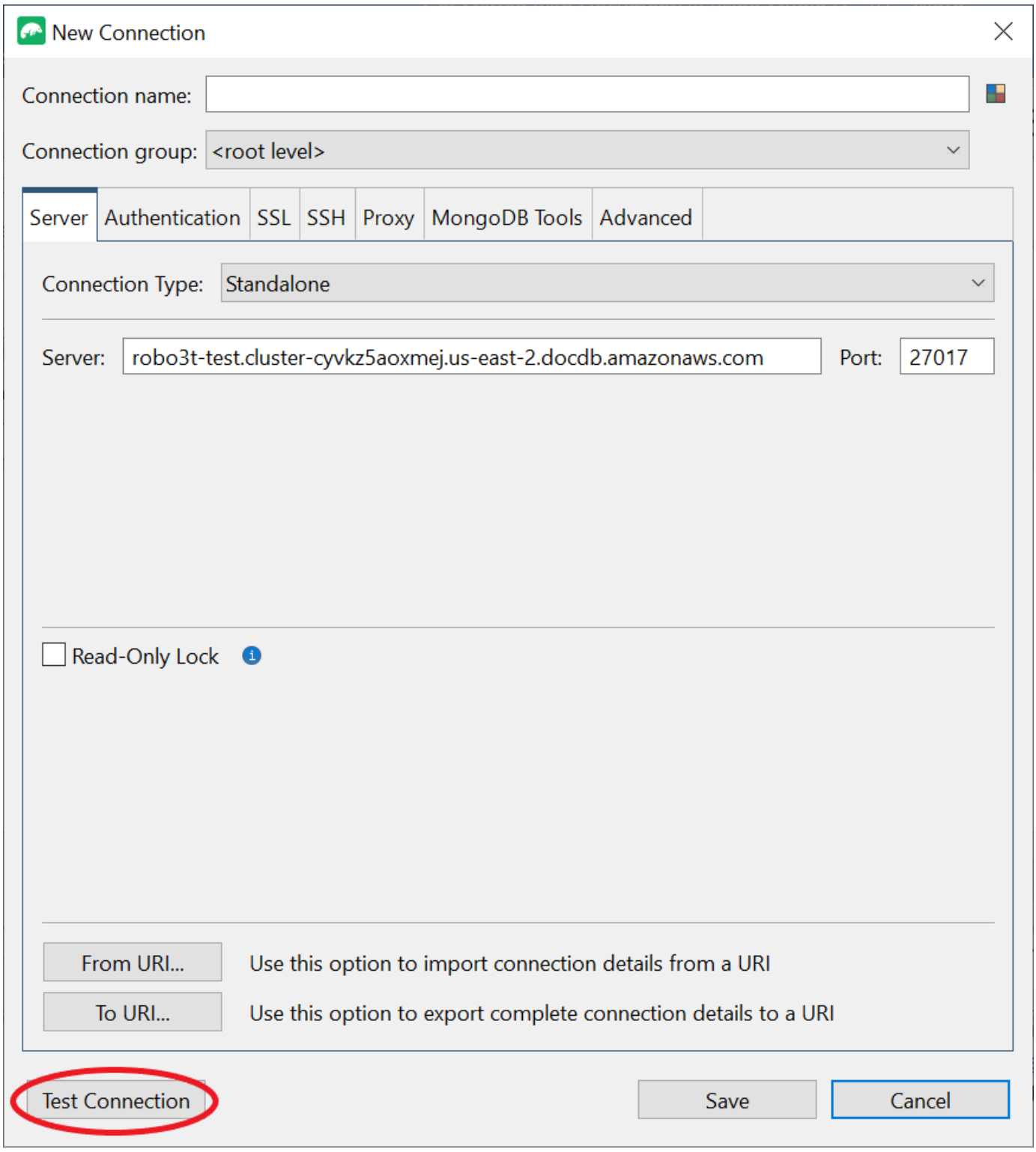
   d. Si está en una máquina cliente Linux/macOS, es posible que deba cambiar los permisos de su clave privada mediante el siguiente comando:

      ```
      chmod 400 /fullPathToYourPemFile/<yourKey>.pem
      ```

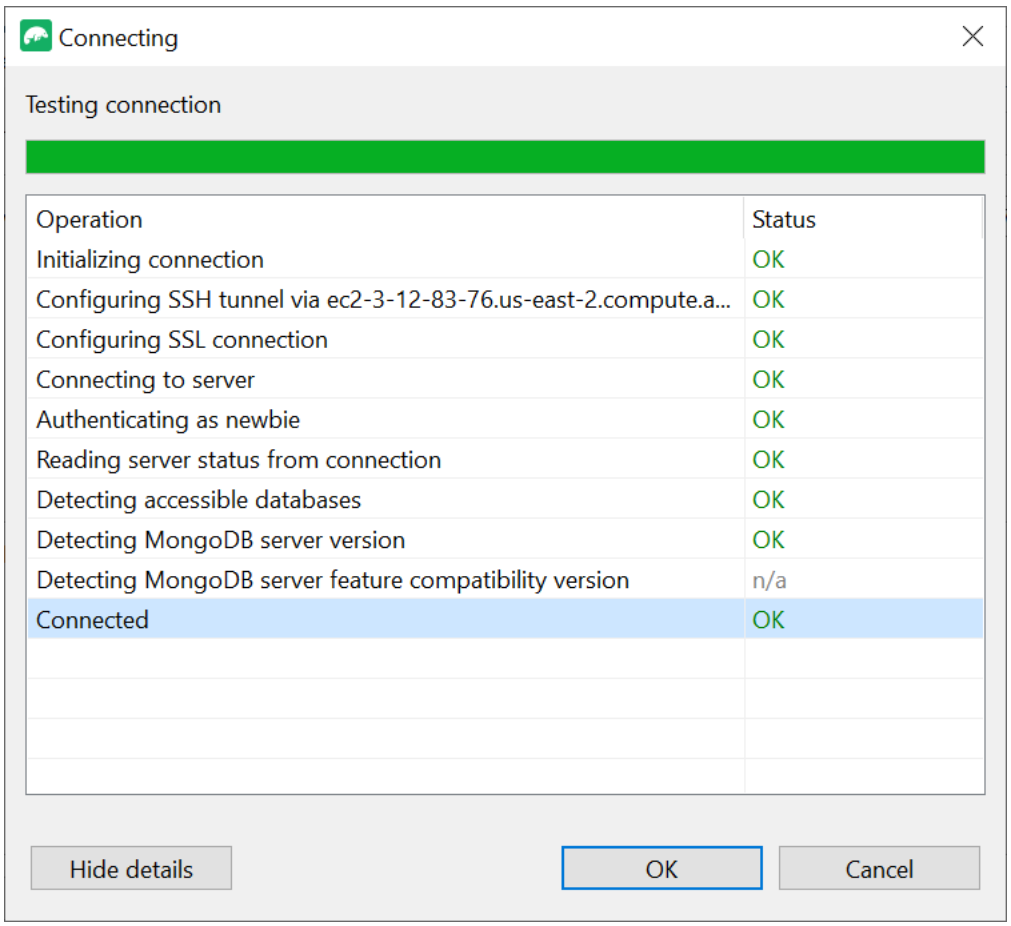


> **Note**
>
> Esta instancia de Amazon EC2 debe estar en la misma VPC de Amazon y grupo de seguridad que el clúster de DocumentDB. Puede obtener la dirección SSH, el nombre de usuario y la clave privada en su Consola de administración de Amazon EC2.

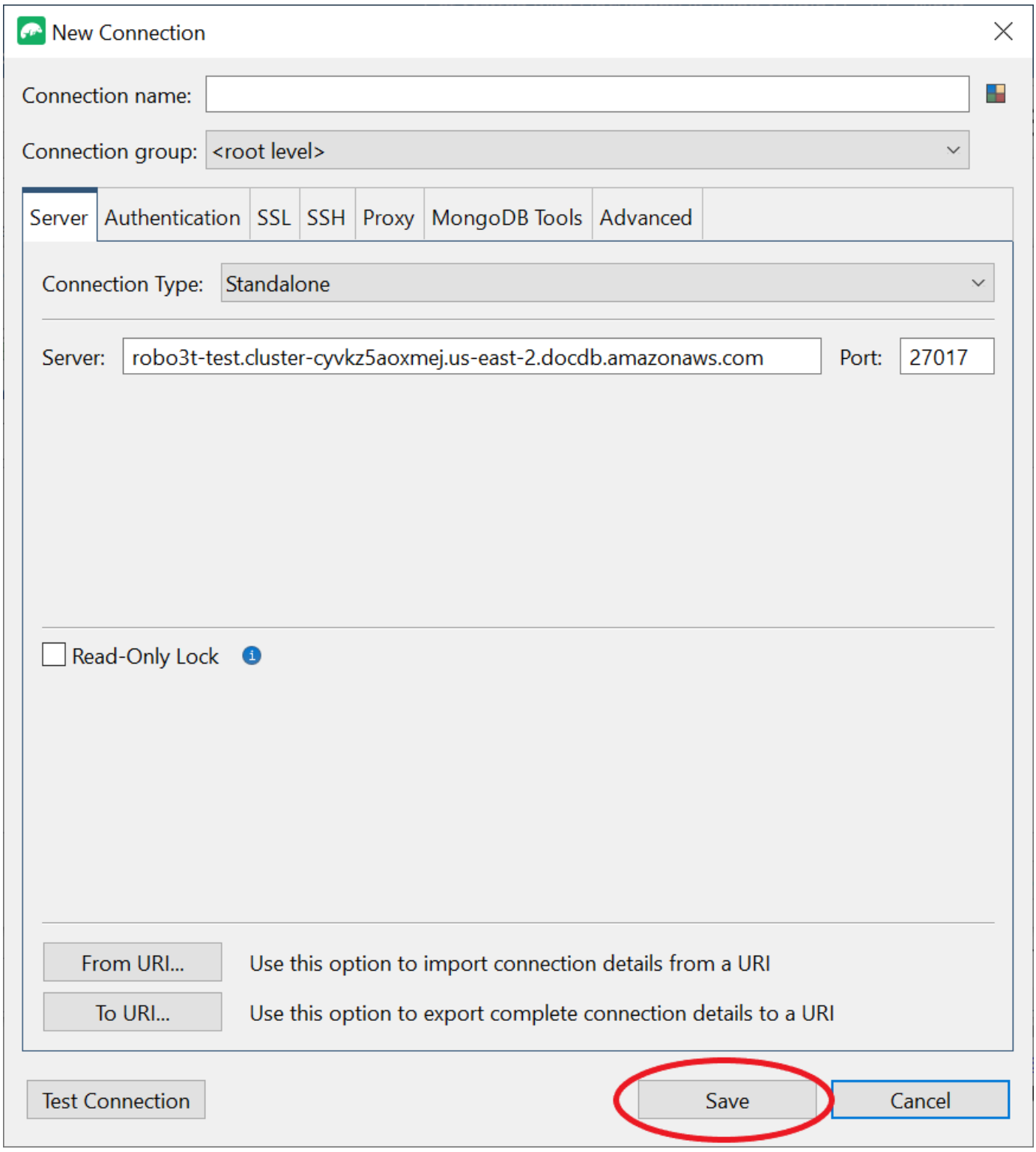
9. Ahora pruebe la configuración pulsando el botón Probar conexión.



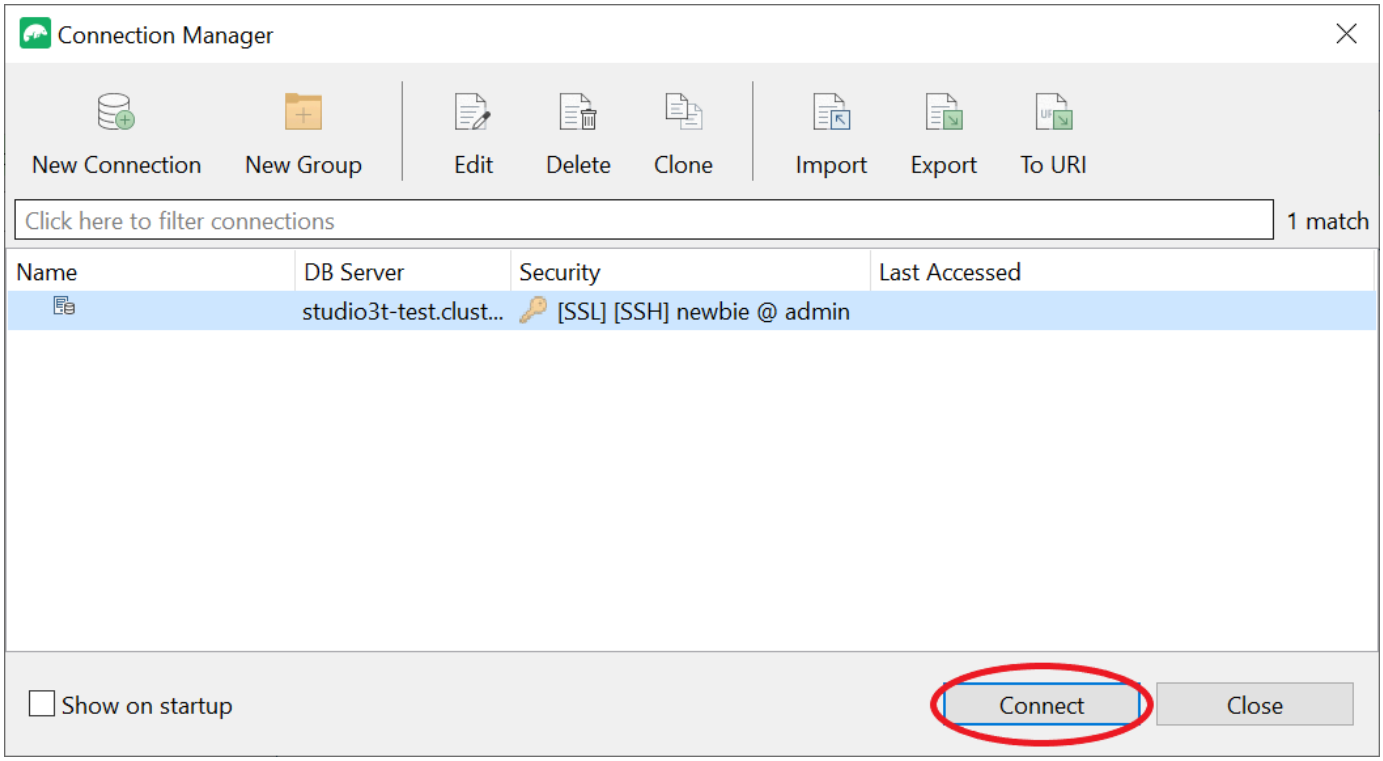
10. Una ventana de diagnóstico debería cargar una barra verde para indicar que la prueba se ha realizado correctamente. Ahora pulse Aceptar para cerrar la ventana de diagnóstico.



11. Elija Guardar para guardar la conexión y usarla en el futuro.



12. Ahora seleccione su clúster y elija Conectar.



¡Enhorabuena! Se ha conectado correctamente a su clúster de Amazon DocumentDB a través de Studio 3T.

Conexión a Amazon DocumentDB mediante DataGrip

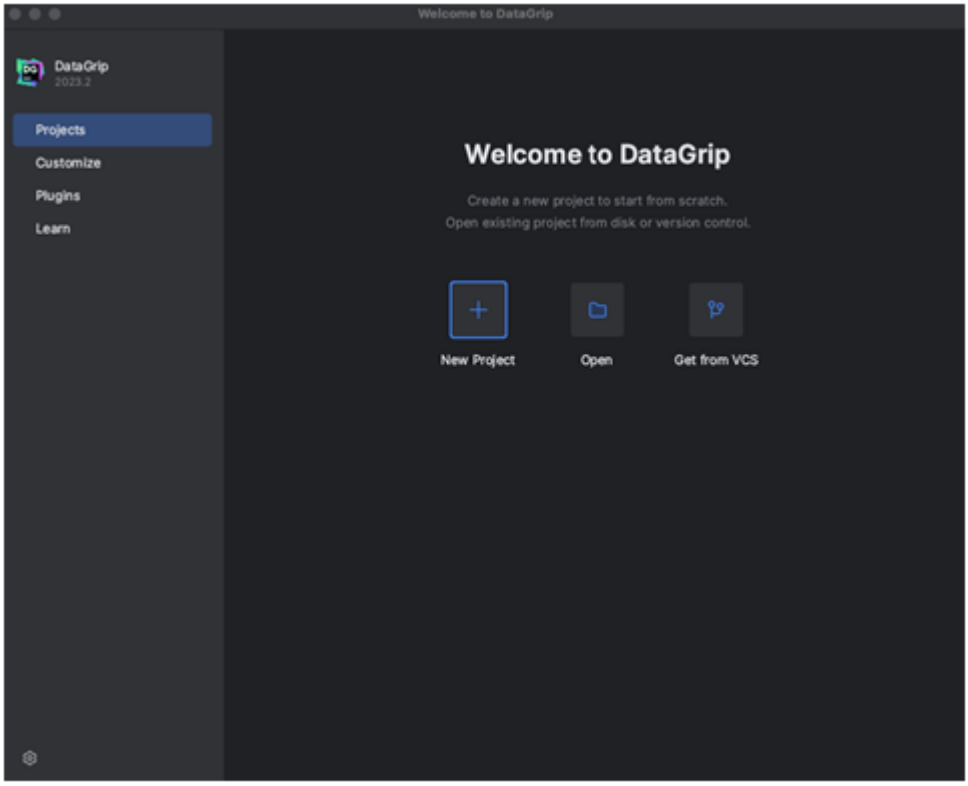
DataGrip es un potente entorno de desarrollo integrado (IDE) que admite varios sistemas de bases de datos, incluido Amazon DocumentDB. En esta sección se explican los pasos para conectarse a su clúster de Amazon DocumentDB mediante DataGrip, lo que le permite administrar y consultar sus datos fácilmente mediante una interfaz gráfica.

Requisitos previos

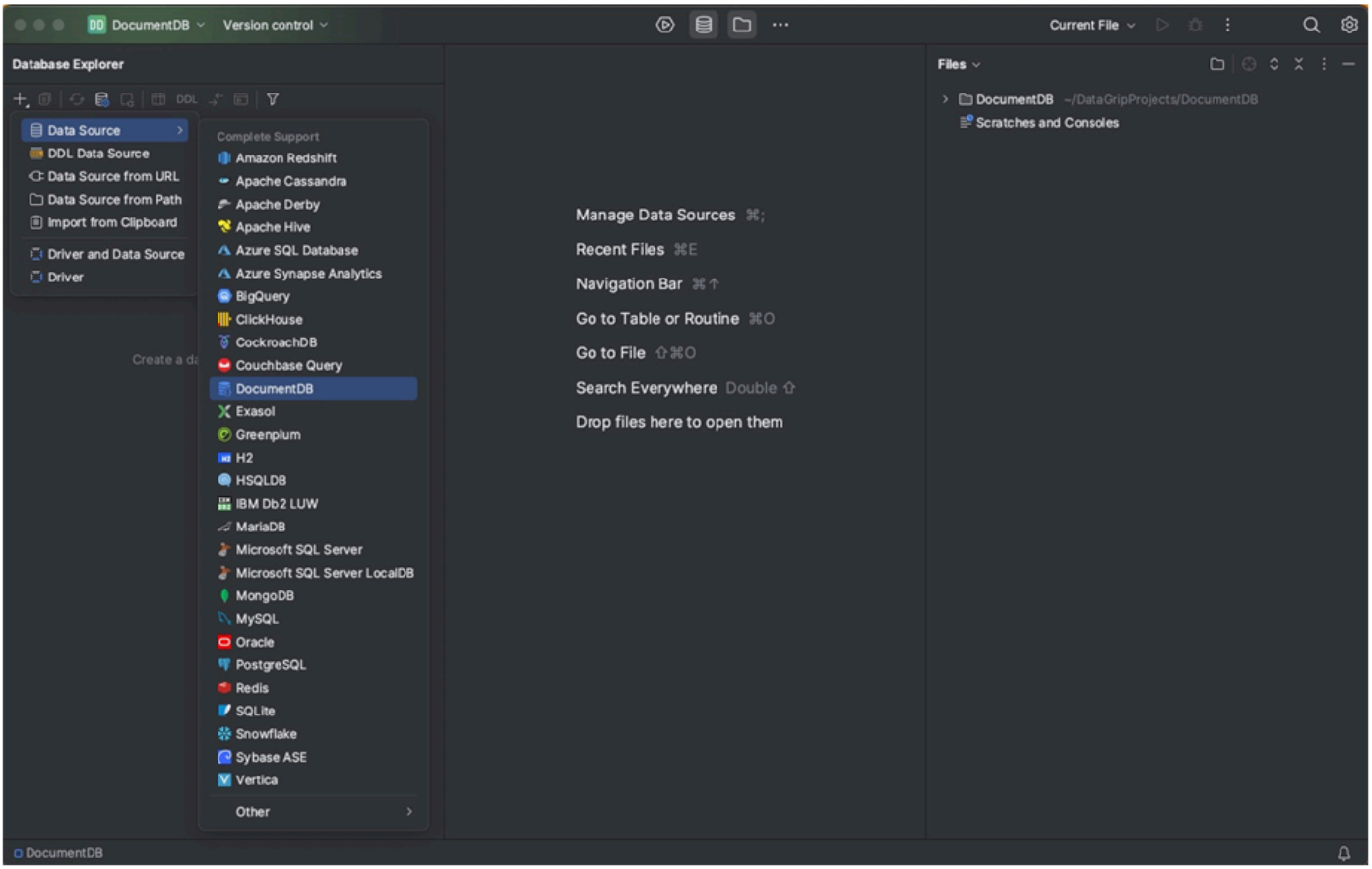
- El IDE de DataGrip está instalado en su máquina. Puede descargarlo desde JetBrains.
- Una instancia de Amazon EC2 que se ejecute en la misma VPC que el clúster de Amazon DocumentDB. Utilizará esta instancia para establecer un túnel seguro desde su máquina local hasta el clúster de Amazon DocumentDBCluster. Siga estas instrucciones sobre cómo Connect mediante Amazon EC2:
- Como alternativa a una instancia Amazon EC2, a una conexión VPN o si ya está accediendo a su infraestructura de AWS mediante una VPN segura. Si prefiere esta opción, siga las instrucciones para acceder de forma segura a Amazon DocumentDB mediante AWS Client VPN.

Conexión mediante DataGrip

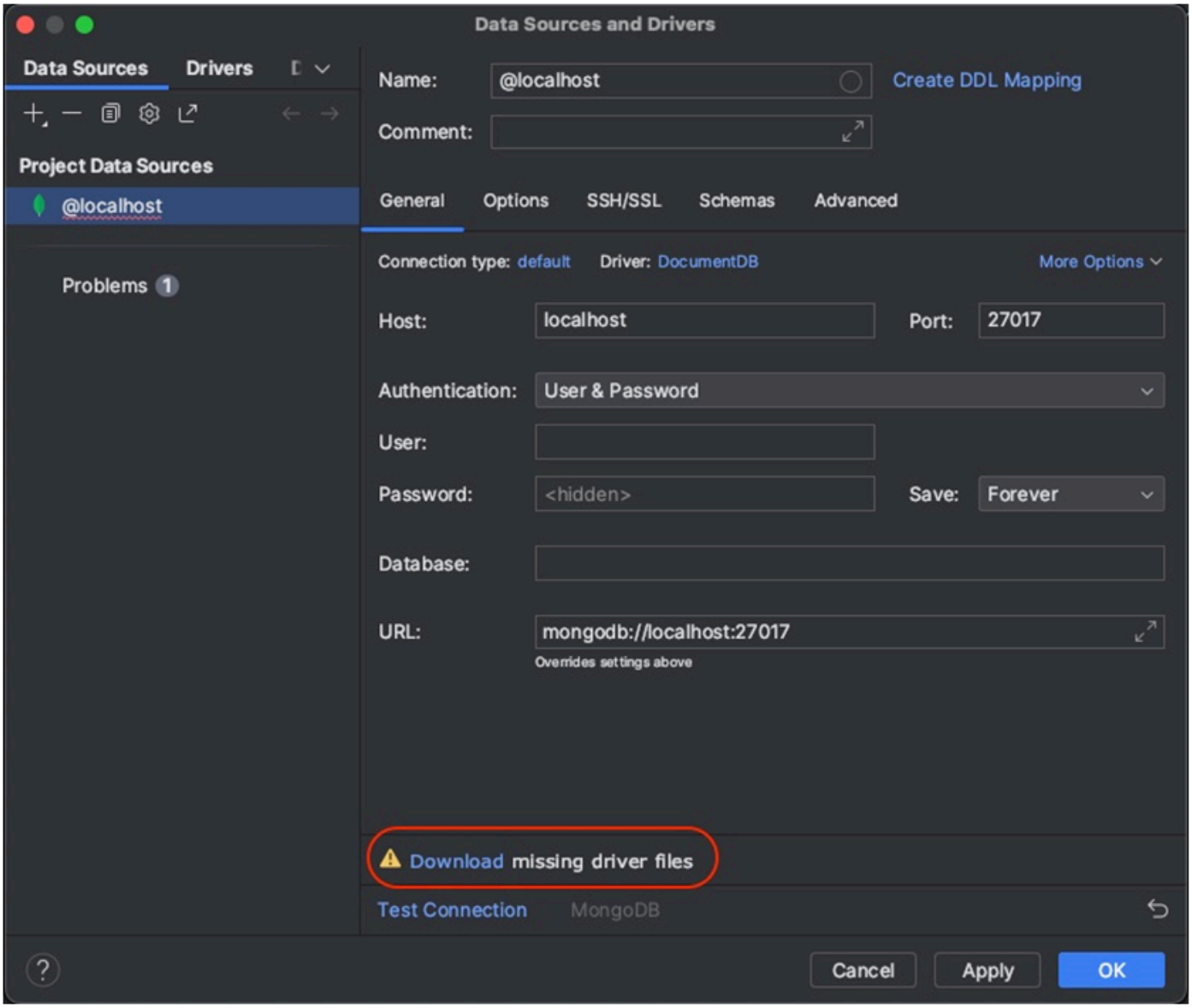
1. Inicie DataGrip en su ordenador y cree un Nuevo proyecto.



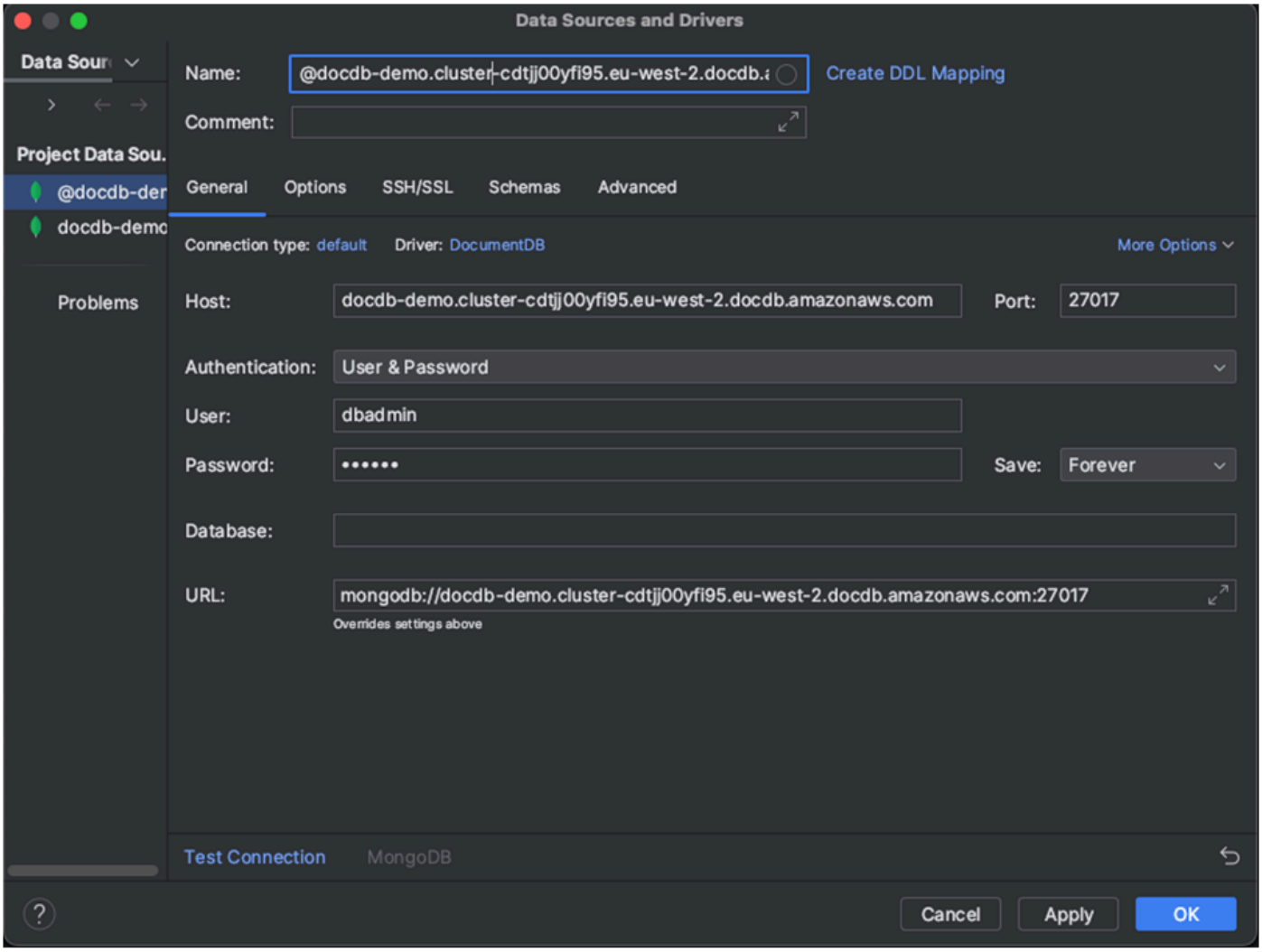
2. Agregue un nuevo origen de datos de una de las siguientes formas:
   a. En el menú principal, vaya a Archivo — Nuevo — Origen de datos y seleccione DocumentDB
   b. En el explorador de bases de datos, haga clic en el nuevo icono (+) de la barra de herramientas. Vaya al origen de datos y seleccione DocumentDB.



3. En la página Orígenes de datos de la pestaña General, compruebe si hay un enlace para descargar los archivos del controlador que faltan en la parte inferior del área de configuración de la conexión. Haga clic en este enlace para descargar los controladores necesarios para interactuar con una base de datos. Para obtener un enlace de descarga directa, consulte los controladores JDBC de JetBrains.

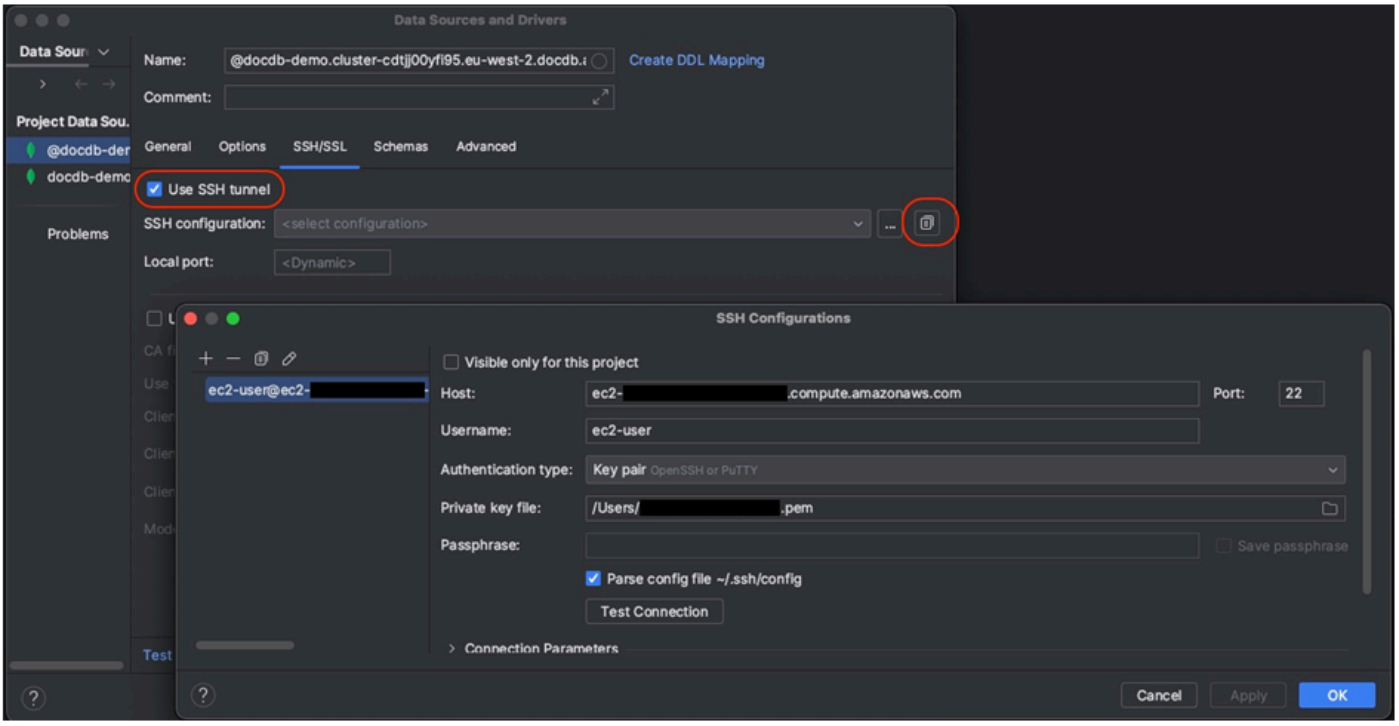


4. En la pestaña General, especifique los detalles de la conexión:
   a. En el campo Host, especifique el punto de conexión del clúster de Amazon DocumentDB.
   b. El puerto ya está establecido en 27017. Cámbielo si el clúster se implementó en un puerto diferente.
   c. En Autenticación, elija Nombre de usuario y contraseña.
   d. Introduzca la información de nombre de usuario y contraseña.
   e. El campo Base de datos es opcional. Puede especificar la base de datos a la que desea conectarse.
   f. El campo URL se completa automáticamente a medida que añade los detalles anteriores.



5. En la pestaña SSH/SSL, habilite Usar túnel SSH y, a continuación, haga clic en el icono para abrir el cuadro de diálogo Configuración de SSH. Introduzca la información siguiente:
   a. En el campo Host, introduzca el nombre de host de su instancia de Amazon EC2.
   b. Introduzca el nombre de usuario y la contraseña de la instancia de Amazon EC2.
   c. En Tipo de autenticación, elija Par de claves.
   d. Introduzca su Archivo de clave privada.

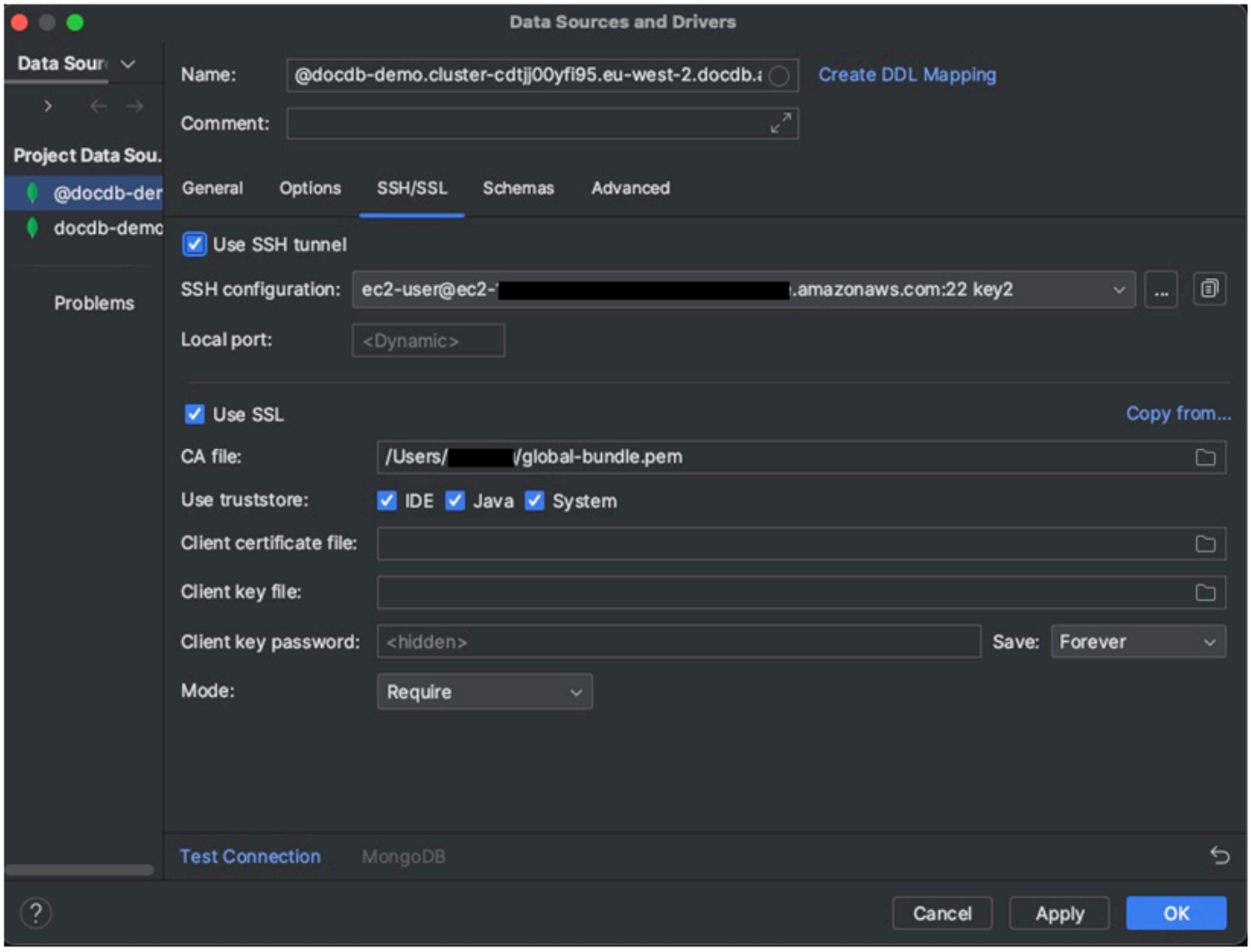
> **Note**
>
> Si utiliza la opción VPN, no es necesario configurar el túnel SSH.



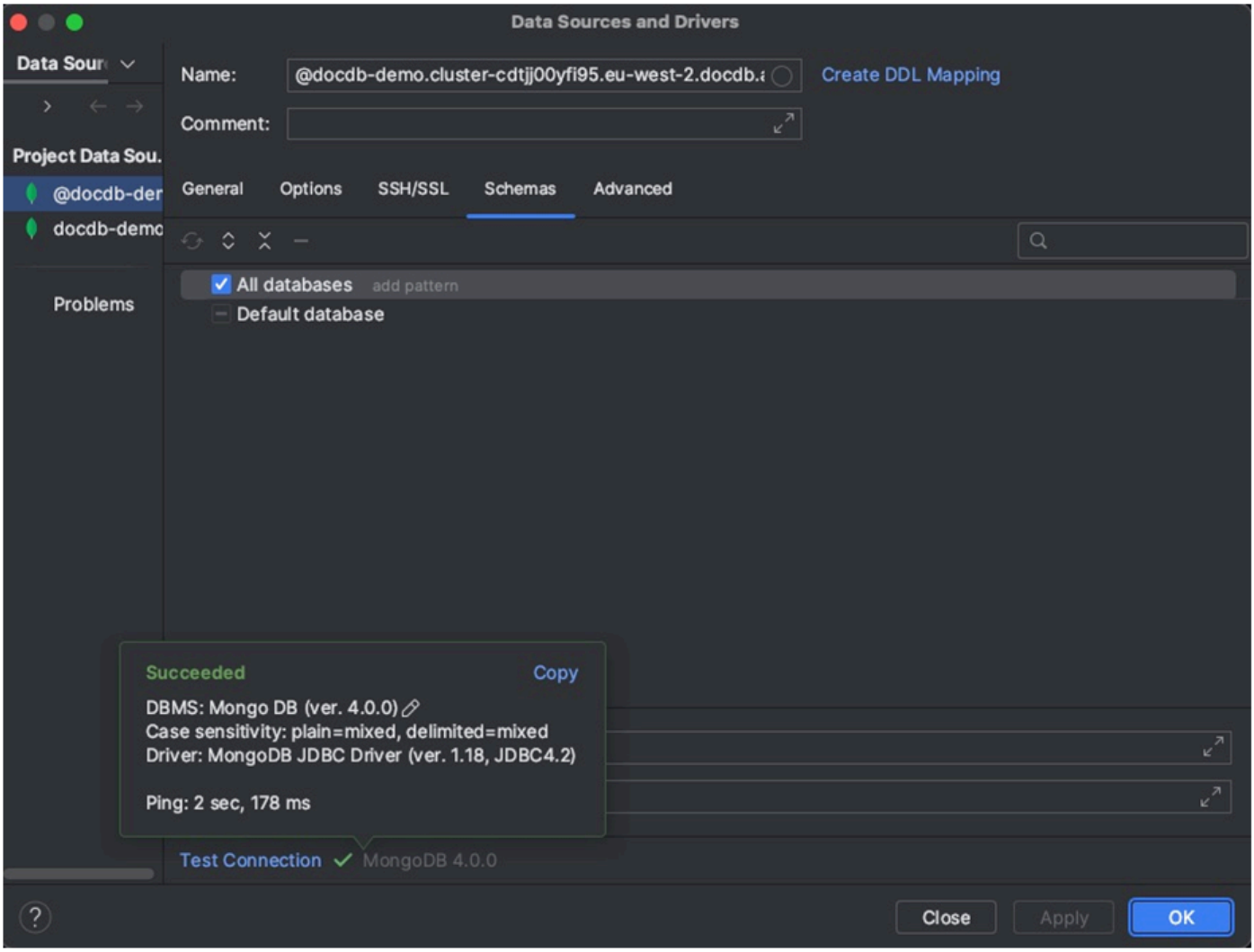
6. En la pestaña SSH/SSL, habilite Usar SSL. En el campo Archivo CA, introduzca la ubicación del archivo `global-bundle.pem` en su ordenador. En Modo, deje la opción Requerir.

> **Note**
>
> Puede descargar el certificado desde esta ubicación o con este comando: wget https://truststore.pki.rds.amazonaws.com/global/global-bundle.pem

> **Note**
>
> Si se está conectando al clúster elástico de Amazon DocumentDB, no tiene que especificar el archivo CA. Deje marcada la opción Usar SSL y todas las demás opciones con sus valores predeterminados.



7. En la pestaña Esquemas, elija Todas las bases de datos o introduzca el filtro “*:*” en el campo del patrón del esquema. Haga clic en el enlace Probar la conexión para probar la conexión.



8. Una vez que la conexión se haya probado correctamente, haga clic en Aceptar para guardar la configuración del origen de datos.

Características de DataGrip

DataGrip ofrece varias características para ayudarle a trabajar con Amazon DocumentDB de forma eficiente:

- Editor de SQL: escriba y ejecute consultas tipo SQL en sus colecciones de DocumentDB mediante el editor SQL de DataGrip.
- Generador visual de consultas: utilice el generador visual de consultas para crear consultas de forma gráfica sin escribir el código SQL.
- Administración de esquemas: administre fácilmente el esquema de su base de datos, incluida la creación, modificación y eliminación de colecciones.

- Visualización de datos: vea y analice sus datos con varias herramientas de visualización disponibles en DataGrip.
- Exportación e importación de datos: transfiera datos entre Amazon DocumentDB y otras bases de datos mediante las características de exportación e importación de DataGrip.

Consulte la documentación oficial de DataGrip para obtener características y consejos más avanzados sobre cómo trabajar con Amazon DocumentDB y otros sistemas de bases de datos.

Connect mediante Amazon EC2

En esta sección se describe cómo configurar la conectividad entre un clúster de Amazon DocumentDB y Amazon EC2 y cómo acceder al clúster de Amazon DocumentDB desde la instancia de Amazon. EC2

Existen dos opciones para configurar la EC2 conexión:

- Conectar automáticamente la EC2 instancia a una base de datos de Amazon DocumentDB: utilice la función de conexión automática de la EC2 consola para configurar automáticamente la conexión entre la EC2 instancia y una base de datos Amazon DocumentDB nueva o existente. Esta conexión permite que el tráfico viaje entre la EC2 instancia y la base de datos Amazon DocumentDB. Esta opción se utiliza normalmente para probar y crear nuevos grupos de seguridad.
- Conectar manualmente la EC2 instancia a la base de datos de Amazon DocumentDB: configure la conexión entre la EC2 instancia y la base de datos de Amazon DocumentDB configurando y asignando manualmente los grupos de seguridad para reproducir la configuración creada por la función de conexión automática. Esta opción se suele utilizar para cambiar configuraciones más avanzadas y usar los grupos de seguridad existentes.

Requisitos previos

Independientemente de la opción y antes de crear el primer clúster de Amazon DocumentDB, debe hacer lo siguiente:

Creación de una cuenta de Amazon Web Services (AWS)

Para empezar a utilizar Amazon DocumentDB, debe tener una cuenta de Amazon Web Services (AWS). La AWS cuenta es gratuita. Solo se paga por los servicios y los recursos que se utilicen.

Si no tiene una Cuenta de AWS, complete los siguientes pasos para crearla.

Para suscribirte a una Cuenta de AWS

1. Abrir https://portal.aws.amazon.com/billing/registro.
2. Siga las instrucciones que se le indiquen.

   Parte del procedimiento de registro consiste en recibir una llamada telefónica o mensaje de texto e indicar un código de verificación en el teclado del teléfono.

   Cuando te registras en un Cuenta de AWS, Usuario raíz de la cuenta de AWSse crea un. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario y utilice únicamente el usuario raíz para realizar Tareas que requieren acceso de usuario raíz.

Si lo desea, configure los permisos AWS Identity and Access Management (IAM) necesarios.

El acceso para gestionar los recursos de Amazon DocumentDB, como clústeres, instancias y grupos de parámetros de clústeres, requiere credenciales que AWS pueda utilizar para autenticar sus solicitudes. Para obtener más información, consulte Identity and Access Management para Amazon DocumentDB.

1. En la barra de búsqueda Consola de administración de AWS, escriba IAM y seleccione IAM en el menú desplegable que aparece.
2. Cuando esté en la consola de IAM, seleccione Usuarios en el panel de navegación.
3. Seleccione su nombre de usuario.
4. Haga clic en el botón Añadir permisos.
5. Seleccione Asociar directamente las políticas existentes.
6. Escriba `AmazonDocDBFullAccess` en la barra de búsqueda y selecciónelo en cuanto aparezca en los resultados de búsqueda.
7. Haga clic en el botón azul de la parte inferior que dice Siguiente: Revisión.
8. Haga clic en el botón azul de la parte inferior que dice Añadir permisos.

Creación de una Amazon Virtual Private Cloud (Amazon VPC)

En función del lugar en el que se Región de AWS encuentre, es posible que ya tenga creada una VPC predeterminada o no. Si no cuenta con una VPC determinada, complete el paso 1 de

la Introducción a Amazon VPC en la Guía del usuario de Amazon VPC. Esto tardará menos de cinco minutos.

Connect Amazon EC2 automáticamente

Temas

- Conectar automáticamente una EC2 instancia a una nueva base de datos de Amazon DocumentDB
- Conectar automáticamente una EC2 instancia a una base de datos Amazon DocumentDB existente
- Descripción general de la conectividad automática con una instancia EC2
- Visualización de los recursos de computación conectados

Antes de configurar una conexión entre una EC2 instancia y una nueva base de datos de Amazon DocumentDB, asegúrese de cumplir los requisitos descritos en. Descripción general de la conectividad automática con una instancia EC2 Si realiza cambios en los grupos de seguridad después de configurar la conectividad, los cambios pueden afectar a la conexión entre la EC2 instancia y la base de datos Amazon DocumentDB.

> **Note**
>
> Solo puede configurar automáticamente una conexión entre una EC2 instancia y una base de datos de Amazon DocumentDB mediante. Consola de administración de AWS No puede configurar una conexión automáticamente con la API AWS CLI o Amazon DocumentDB.

Conectar automáticamente una EC2 instancia a una nueva base de datos de Amazon DocumentDB

En el siguiente proceso se presupone que ha completado los pasos que se detallan en el tema Requisitos previos.

Steps

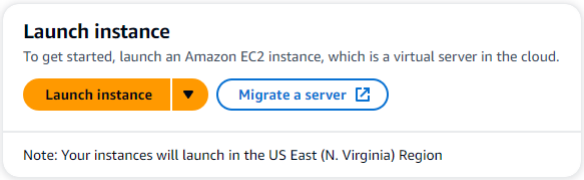
- Paso 1: Crear una EC2 instancia de Amazon
- Paso 2: creación de un clúster de Amazon DocumentDB
- Paso 3: Conéctate a tu EC2 instancia de Amazon
- Paso 4: instalación del intérprete de comandos de MongoDB

- Paso 5: administración de TLS de Amazon DocumentDB
- Paso 6: conexión al clúster de Amazon DocumentDB
- Paso 7: inserción y consulta de datos
- Paso 8: exploración

Paso 1: Crear una EC2 instancia de Amazon

En este paso, creará una EC2 instancia de Amazon en la misma región y Amazon VPC que utilizará más adelante para aprovisionar el clúster de Amazon DocumentDB.

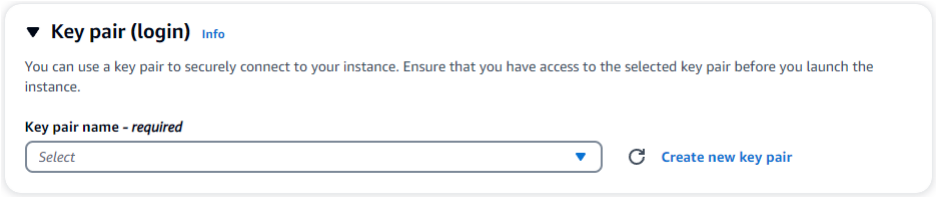
1. En la EC2 consola de Amazon, selecciona Launch instance.



2. Ingrese un nombre o identificador en el campo Nombre ubicado en la sección Nombres y etiquetas.
3. En la lista desplegable Imagen de máquina de Amazon (AMI), busque la AMI de Amazon Linux 2 y selecciónela.



4. Busque y seleccione t3.micro en la lista desplegable de Tipo de instancia.
5. En la sección Par de claves (inicio de sesión), ingrese el identificador de un par de claves existente o elija Crear un par de claves nuevo.



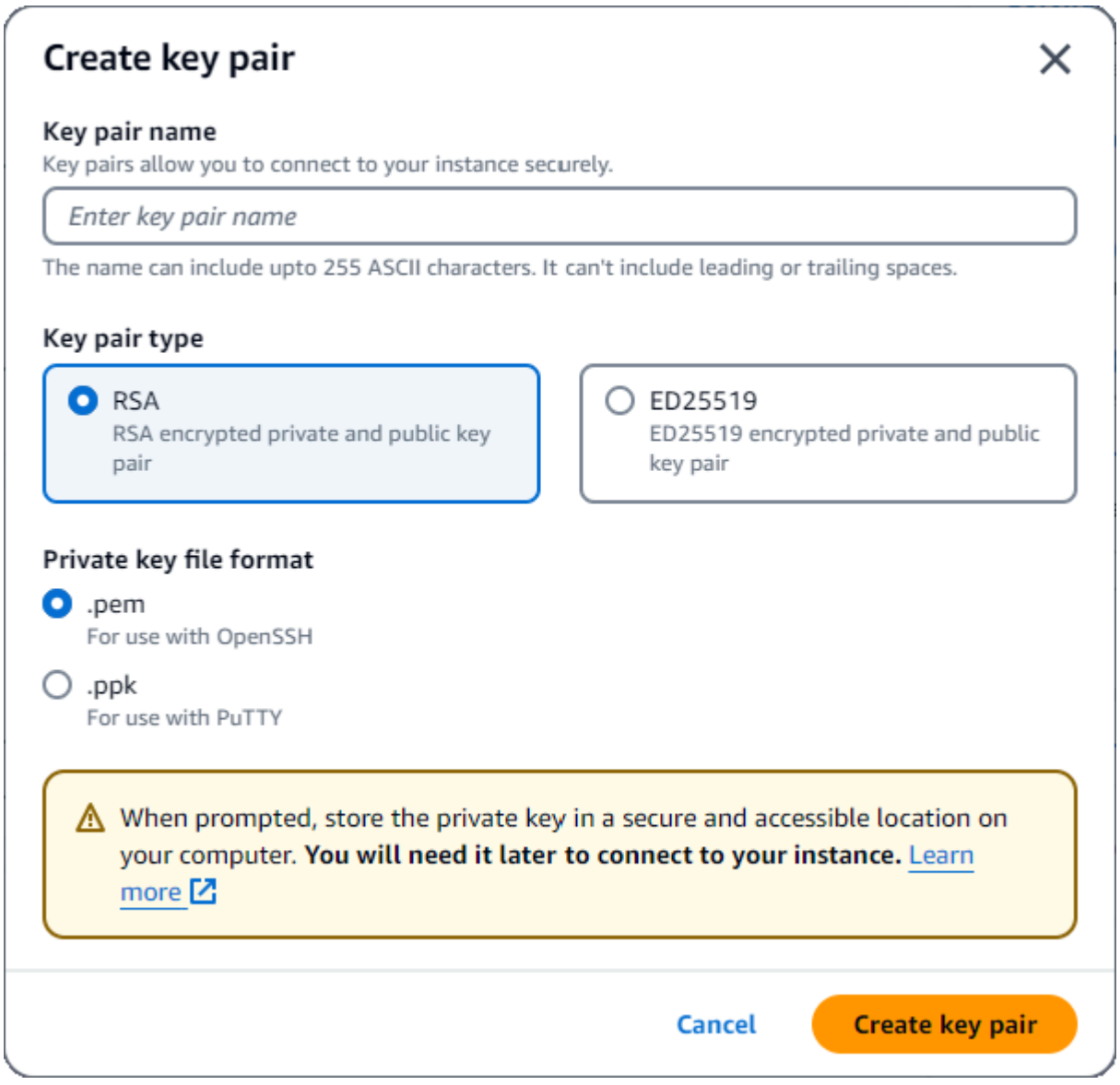
Debes proporcionar un EC2 key pair de Amazon.

- Si tienes un par de EC2 claves de Amazon:
  1. Seleccione un par de claves, elija su par de claves de la lista.

2. Debes tener ya disponible el archivo de clave privada (archivo.pem o.ppk) para iniciar sesión en tu instancia de Amazon. EC2

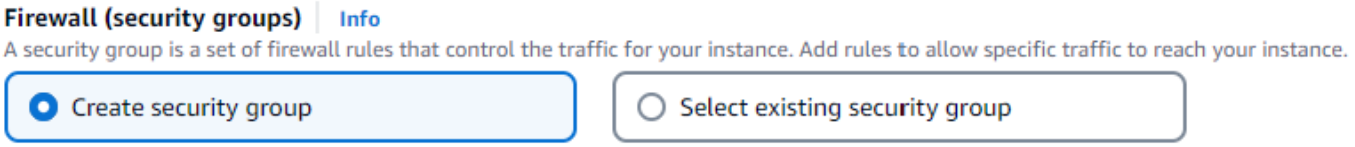
- Si no tienes un par de EC2 claves de Amazon:

1. Seleccione Crear un par de claves nuevo y aparecerá el cuadro de diálogo Crear par de claves.
2. Escriba un nombre en el campo Nombre del par de claves.
3. Seleccione el Tipo de par de claves y el Formato de archivo de clave privada.
4. Elija Crear par de claves.



> **Note**
>
> Por motivos de seguridad, te recomendamos encarecidamente que utilices un par de claves para la conectividad SSH y a Internet con tu instancia. EC2

6. Opcional: en la sección Configuración de red, en Firewall (grupos de seguridad), seleccione Crear grupo de seguridad.



   Elige Crear grupo de seguridad (comprueba todas las reglas de tráfico permitidas que se apliquen a tu EC2 conectividad).

> **Note**
>
> Si desea utilizar un grupo de seguridad existente, siga las instrucciones de Connect Amazon EC2 manualmente.

7. En la sección Resumen, revise la EC2 configuración y, si es correcta, elija Launch instance.

Paso 2: creación de un clúster de Amazon DocumentDB

Mientras se aprovisiona la EC2 instancia de Amazon, cree su clúster de Amazon DocumentDB.

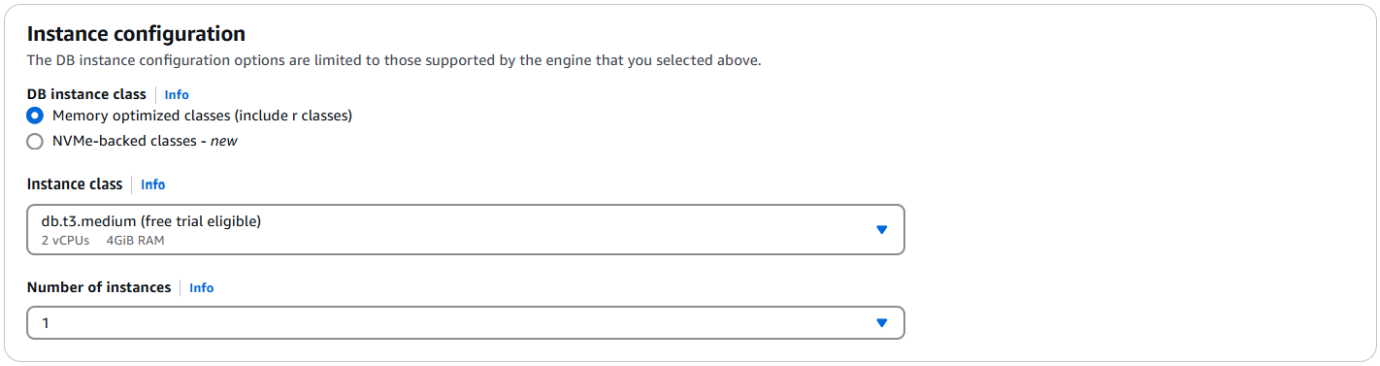
1. Navegue hasta la consola de Amazon DocumentDB y elija Clústeres en el panel de navegación.
2. Seleccione Crear.
3. Deje la configuración de Tipo de clúster como predeterminada en Clúster basado en instancias.
4. En Configuración del clúster, ingrese un nombre único en Identificador de clúster. Tenga en cuenta que la consola cambiará todos los nombres de los clústeres a minúsculas independientemente de cómo se ingresen.

   Deje Versión del motor con su valor predeterminado de 5.0.0.
5. En Configuración del almacenamiento en clúster, deje la configuración predeterminada de Amazon DocumentDB estándar.
6. En Configuración de instancias:

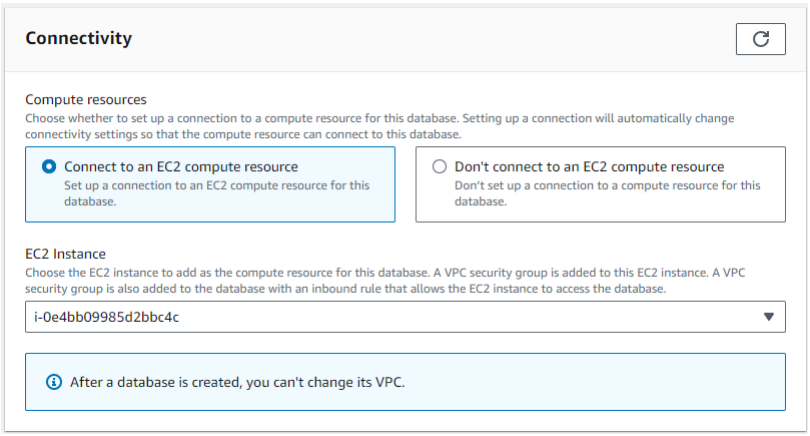
- En Clase de instancia de base de datos, elija Clases optimizadas para memoria (incluidas las clases r), que es la opción predeterminada.

  La otra opción de instancia son las clases respaldadas por NVMecomandos. Para obtener más información, consulte Instancias respaldadas por NVMe.

- En Clase de instancia, elija el tipo de instancia que se adapte a sus necesidades. Para obtener una explicación más detallada de las clases de instancia, consulte Especificaciones de clases de instancias.
- En Número de instancias, elija el número que mejor refleje sus necesidades. Recuerde que cuanto menor sea el número, menor será el costo y menor será el read/write volumen que puede administrar el clúster.



7. En Conectividad, elija Conectarse a un recurso EC2 informático. Esta es la EC2 instancia que creaste en el paso 1.



> **Note**
>
> La conexión a un recurso EC2 informático crea automáticamente un grupo de seguridad para la conexión del recurso EC2 informático al clúster de Amazon DocumentDB. Cuando haya terminado de crear el clúster y desee ver el grupo de seguridad recién creado, navegue hasta la lista de clústeres y elija el identificador del clúster. En la pestaña Conectividad y seguridad, vaya a Grupos de seguridad y busque su grupo en Nombre del grupo de seguridad (ID). Contendrá el nombre del clúster y tendrá un aspecto similar al siguiente: `docdb-ec2-docdb-2023-12-11-21-33-41:i-0e4bb09985d2bbc4c (sg-0238e0b0bf0f73877)`.

8. En la sección Autenticación, ingrese un nombre de usuario para el usuario principal y, a continuación, elija Autoadministrado. Ingrese una contraseña y, a continuación, confírmela.

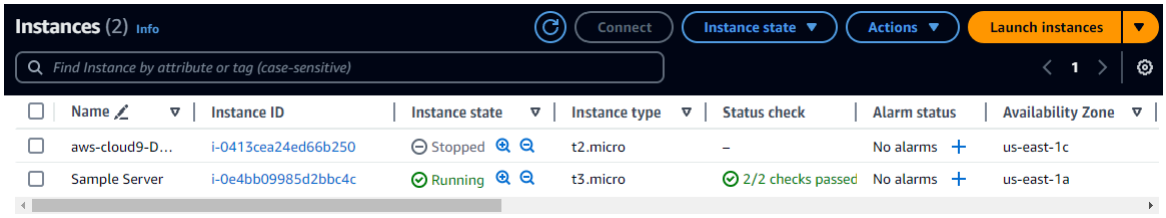
   Si, en su lugar, eligió Administrado en AWS Secrets Manager, consulte Administración de contraseñas con Amazon DocumentDB y AWS Secrets Manager para obtener más información.

9. Elija Create cluster.

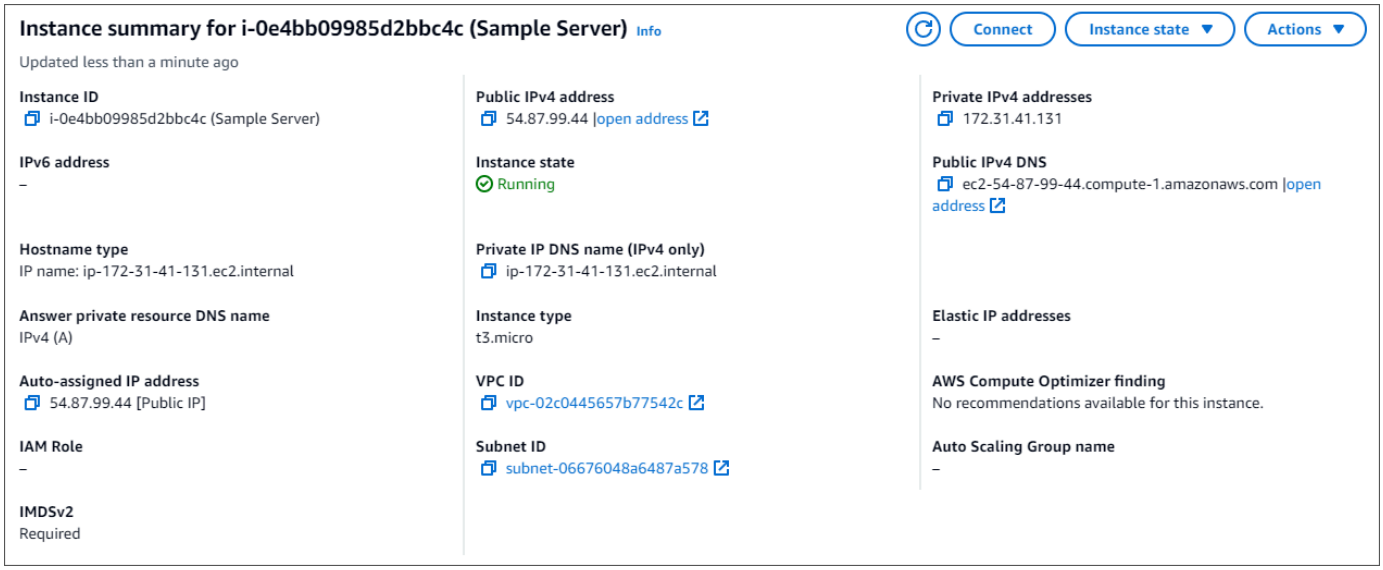
Paso 3: Conéctate a tu EC2 instancia de Amazon

Para instalar el shell mongo, primero debes conectarte a tu EC2 instancia de Amazon. La instalación del intérprete de comandos de mongo permite conectarse a su clúster de Amazon DocumentDB y realizar consultas en él. Realice los siguientes pasos:

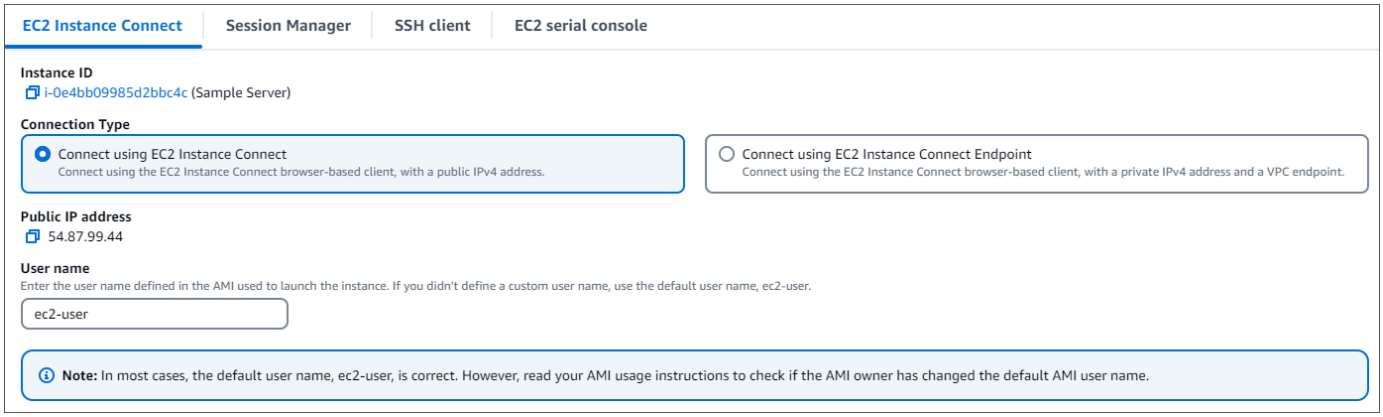
1. En la EC2 consola de Amazon, navega hasta tus instancias y comprueba si la instancia que acabas de crear se está ejecutando. Si es así, haga clic en el ID de la instancia para seleccionar la instancia.



2. Elija Conectar.



3. Existen cuatro opciones con pestañas para su método de conexión: Amazon EC2 Instance Connect, Session Manager, cliente SSH o consola EC2 serie. Debe elegir uno y seguir sus instrucciones. Cuando haya terminado, elija Conectar.



> **Note**
>
> Si su dirección IP ha cambiado después de iniciar este tutorial o si va a volver a su entorno más adelante, debe actualizar la regla de entrada del grupo de seguridad `demoEC2` para habilitar el tráfico entrante desde su nueva dirección de API.

Paso 4: instalación del intérprete de comandos de MongoDB

Ahora puede instalar el intérprete de comandos de MongoDB, que es una utilidad de línea de comandos que se utiliza para conectarse al clúster de Amazon DocumentDB y consultarlo.

Actualmente hay dos versiones del intérprete de comandos de MongoDB: la versión más reciente, mongosh, y la versión anterior, el intérprete de comandos de mongo.

> **Important**
>
> Existe una limitación conocida con los controladores de Node.js anteriores a la versión 6.13.1, ya que Amazon DocumentDB no los admite actualmente para la autenticación de identidad de IAM. Los controladores Node.js y las herramientas que utilizan el controlador Node.js (como mongosh) deben actualizarse al controlador Node.js versión 6.13.1 o posterior.

Siga las siguientes instrucciones para instalar el intérprete de comandos de MongoDB en su sistema operativo.

On Amazon Linux

Cómo instalar el intérprete de comandos de MongoDB en Amazon Linux

Si no utiliza la autenticación de IAM y desea utilizar el último intérprete de comandos de MongoDB (mongosh) para conectarse a su clúster de Amazon DocumentDB, siga estos pasos:

1. Cree el archivo de repositorio. En la línea de comandos de la EC2 instancia que creó, ejecute el siguiente comando:

   ```
   echo -e "[mongodb-org-5.0] \nname=MongoDB Repository\nbaseurl=https://
   repo.mongodb.org/yum/amazon/2023/mongodb-org/5.0/x86_64/\ngpgcheck=1 \nenabled=1
    \ngpgkey=https://pgp.mongodb.com/server-5.0.asc" | sudo tee /etc/yum.repos.d/
   mongodb-org-5.0.repo
   ```

2. Cuando esté completo, instale mongosh con una de las siguientes opciones de comando en el símbolo del sistema:

   Opción 1: si eligió el Amazon Linux 2023 predeterminado durante la EC2 configuración de Amazon, introduzca este comando:

   ```
   sudo yum install -y mongodb-mongosh-shared-openssl3
   ```

   Opción 2: si eligió Amazon Linux 2 durante la EC2 configuración de Amazon, introduzca este comando:

```
sudo yum install -y mongodb-mongosh
```

Si utiliza la autenticación de IAM, debe utilizar la versión anterior del intérprete de comandos de MongoDB (5.0) para conectarse al clúster de Amazon DocumentDB. Siga estos pasos:

1. Cree el archivo de repositorio. En la línea de comandos de la EC2 instancia que creó, ejecute el siguiente comando:

```
echo -e "[mongodb-org-5.0] \nname=MongoDB Repository\nbaseurl=https://
repo.mongodb.org/yum/amazon/2023/mongodb-org/5.0/x86_64/\ngpgcheck=1 \nenabled=1
 \ngpgkey=https://pgp.mongodb.com/server-5.0.asc" | sudo tee /etc/yum.repos.d/
mongodb-org-5.0.repo
```

2. Cuando esté completo, instale el intérprete de comandos de MongoDB 5.0 con la siguiente opción de comando en el símbolo del sistema:

```
sudo yum install -y mongodb-org-shell
```

On Ubuntu

Cómo instalar mongosh en Ubuntu

1. Importe la clave pública que utilizará el sistema de administración de paquetes.

```
curl -fsSL https://pgp.mongodb.com/server-5.0.asc | sudo gpg --dearmor -o /usr/
share/keyrings/mongodb-server-5.0.gpg
```

2. Cree el archivo de lista `mongodb-org-5.0.list` para MongoDB mediante el comando correspondiente a su versión de Ubuntu.

```
echo "deb [ arch=amd64,arm64 signed-by=/usr/share/keyrings/mongodb-
server-5.0.gpg ] https://repo.mongodb.org/apt/ubuntu focal/mongodb-org/5.0
 multiverse" | sudo tee /etc/apt/sources.list.d/mongodb-org-5.0.list
```

3. Importe y actualice la base de datos del paquete local utilizando el siguiente comando:

```
sudo apt-get update
```

4. Instale mongosh.

```
sudo apt-get install -y mongodb-mongosh
```

Para obtener información sobre cómo instalar las versiones anteriores de MongoDB en un sistema Ubuntu, consulte Install MongoDB Community Edition on Ubuntu.

On other operating systems

Para instalar el intérprete de comandos de mongo en otros sistemas operativos, consulte el tema sobre cómo instalar MongoDB Community Edition en la documentación de MongoDB.

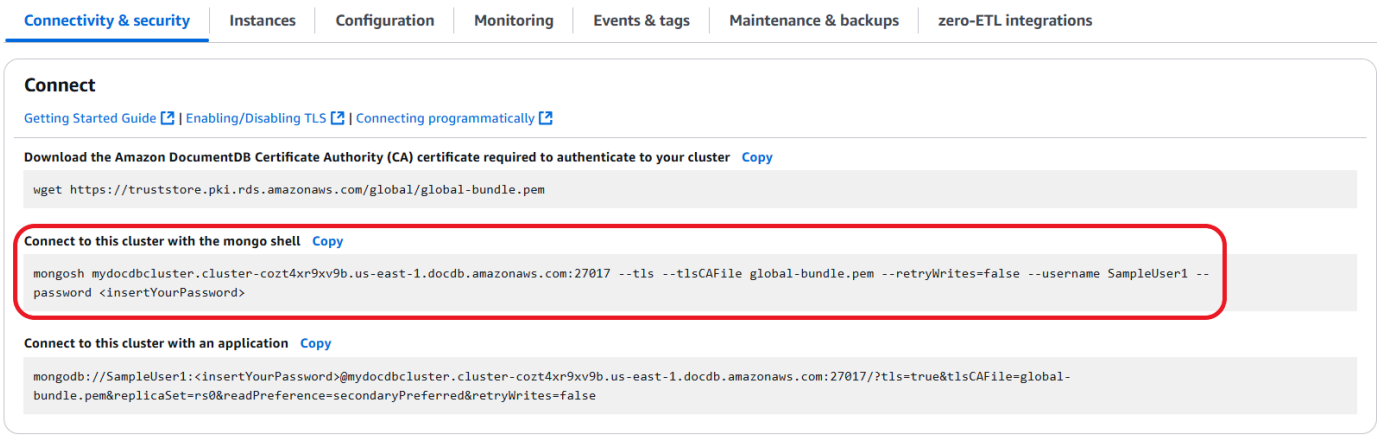
Paso 5: administración de TLS de Amazon DocumentDB

Descargue el certificado CA para Amazon DocumentDB con el siguiente código: `wget https://truststore.pki.rds.amazonaws.com/global/global-bundle.pem`

> **Note**
>
> La seguridad de la capa de transporte (TLS) está habilitada de forma predeterminada para todos los clústeres nuevos de Amazon DocumentDB. Para obtener más información, consulte Managing Amazon DocumentDB cluster TLS settings.

Paso 6: conexión al clúster de Amazon DocumentDB

1. En la consola de Amazon DocumentDB, en Clústeres, localice su clúster. Haga clic en Identificador del clúster para elegir el clúster que creó.
2. En la pestaña Conectividad y seguridad, busque Conectar a este clúster con el intérprete de comandos de mongo en el cuadro Conectar:



Copie la cadena de conexión proporcionada y péguela en el terminal.

Haga los siguientes cambios en ella:

a. Asegúrese de que tenga el nombre de usuario correcto en la cadena.
b. Omita `<insertYourPassword>` para que el intérprete de comandos de mongo le pida la contraseña cuando se conecte.
c. Opcional: si utiliza la autenticación de IAM o utiliza la versión anterior del intérprete de comandos de MongoDB, modifique la cadena de conexión de la siguiente manera:

```
mongo --ssl --host mydocdbcluster.cluster-cozt4xr9xv9b.us-east-1.docdb.amazonaws.com:27017 --sslCAFile global-bundle.pem --username SampleUser1 --password
```

Sustituya `mydocdbcluster.cluster-cozt4xr9xv9b.us-east-1` por la misma información de su clúster.

3. Pulse Intro en el terminal. Ahora se le solicitará la contraseña. Introduzca su contraseña.
4. Cuando introduzca la contraseña y pueda ver el mensaje `rs0 [direct: primary] <env-name>>`, significa que se ha conectado correctamente a su clúster de Amazon DocumentDB.

¿Tiene problemas para conectarse? Consulte Solución de problemas de Amazon DocumentDB.

Paso 7: inserción y consulta de datos

Ahora que está conectado a su clúster, puede realizar algunas consultas para familiarizarse con el uso de una base de datos de documentos.

1. Para insertar un solo documento, escriba lo siguiente:

```
db.collection.insertOne({"hello":"DocumentDB"})
```

Obtiene el siguiente resultado:

```
{
  acknowledged: true,
  insertedId: ObjectId('673657216bdf6258466b128c')
}
```

2. Puede leer el documento que escribió con el comando `findOne()` (ya que solo devuelve un documento). La siguiente entrada:

```
db.collection.findOne()
```

Obtiene el siguiente resultado:

```
{ "_id" : ObjectId("5e401fe56056fda7321fbd67"), "hello" : "DocumentDB" }
```

3. Para realizar algunas consultas más, plantéese un caso de uso de perfiles de juegos. Primero, inserte algunas entradas en una colección titulada `profiles`. La siguiente entrada:

```
db.profiles.insertMany([{ _id: 1, name: 'Matt', status: 'active', level: 12, score:
 202 },
      { _id: 2, name: 'Frank', status: 'inactive', level: 2, score: 9 },
      { _id: 3, name: 'Karen', status: 'active', level: 7, score: 87 },
      { _id: 4, name: 'Katie', status: 'active', level: 3, score: 27 }
])
```

Obtiene el siguiente resultado:

```
{ acknowledged: true, insertedIds: { '0': 1, '1': 2, '2': 3, '3': 4 } }
```

4. Utilice el comando `find()` para devolver todos los documentos de la colección de perfiles. La siguiente entrada:

```
db.profiles.find()
```

Obtendrás un resultado que coincidirá con los datos que escribiste en el paso 3.

5. Utilice una consulta para un único documento mediante un filtro. La siguiente entrada:

```
db.profiles.find({name: "Katie"})
```

   Obtiene el siguiente resultado:

```
{ "_id" : 4, "name" : "Katie", "status": "active", "level": 3, "score":27}
```

6. Ahora intentemos buscar un perfil y modificarlo con el comando `findAndModify`. Le daremos al usuario Matt 10 puntos adicionales con el siguiente código:

```
db.profiles.findAndModify({
        query: { name: "Matt", status: "active"},
        update: { $inc: { score: 10 } }
    })
```

   Se obtiene el siguiente resultado (tenga en cuenta que la puntuación aún no ha aumentado):

```
{
    [{_id : 1, name : 'Matt', status: 'active', level: 12, score: 202}]
```

7. Puede comprobar que su puntuación ha cambiado con la siguiente consulta:

   `db.profiles.find({name: "Matt"})`

   Obtiene el siguiente resultado:

```
{ "_id" : 1, "name" : "Matt", "status" : "active", "level" : 12, "score" : 212 }
```

Paso 8: exploración

¡Enhorabuena! Ha completado correctamente la Guía de inicio rápido para Amazon DocumentDB.

Pasos siguientes Descubra cómo aprovechar al máximo esta potente base de datos con algunas de sus características más populares:

- Administración de Amazon DocumentDB
- Escalado
- Copia de seguridad y restauración

> **Note**
>
> Para ahorrar costos, puede detener el clúster de Amazon DocumentDB para reducir los costos o eliminar el clúster. De forma predeterminada, tras 30 minutos de inactividad, su AWS Cloud9 entorno detendrá la EC2 instancia de Amazon subyacente.

Conectar automáticamente una EC2 instancia a una base de datos Amazon DocumentDB existente

El siguiente procedimiento supone que tiene un clúster de Amazon DocumentDB y una instancia de Amazon EC2 existentes.

Acceda a su clúster de Amazon DocumentDB y configure la conexión con Amazon EC2

1. Acceda al clúster de Amazon DocumentDB.

    a. Inicie sesión en y abra la Consola de administración de AWS consola de Amazon DocumentDB en https://console.aws.amazon.com /docdb.

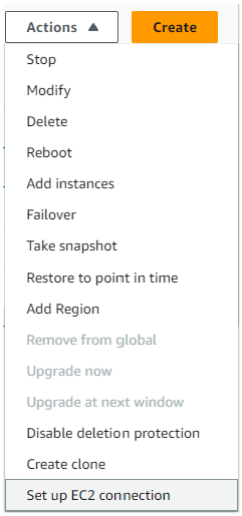
    b. En el panel de navegación, seleccione Clusters (Clústeres).

    > **Tip**
    >
    > Si no ve el panel de navegación del lado izquierdo de la pantalla, seleccione el icono de menú
    > (≡)
    > en la esquina superior izquierda de la página.

    c. Para especificar el clúster que desea, seleccione el botón situado a la izquierda del nombre del clúster.

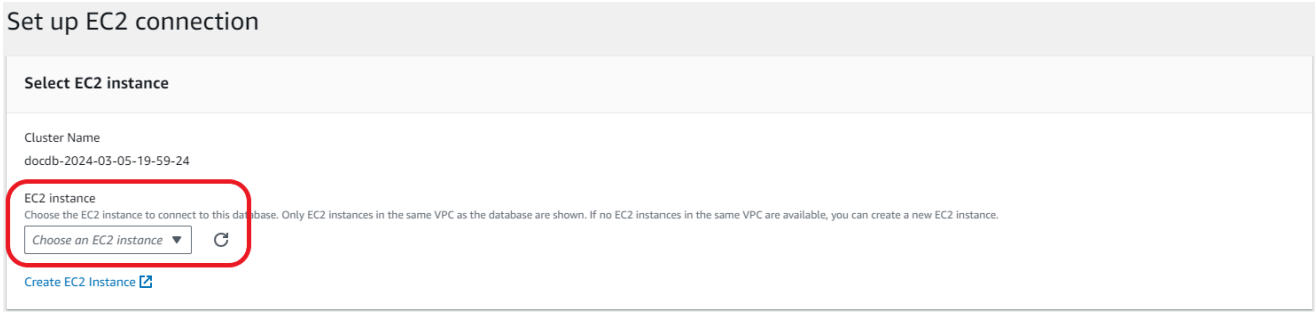
2. Configura la EC2 conexión con Amazon.

    a. Selecciona Acciones y, a continuación, selecciona Configurar EC2 conexión.



Aparece el cuadro de diálogo Configurar la EC2 conexión.

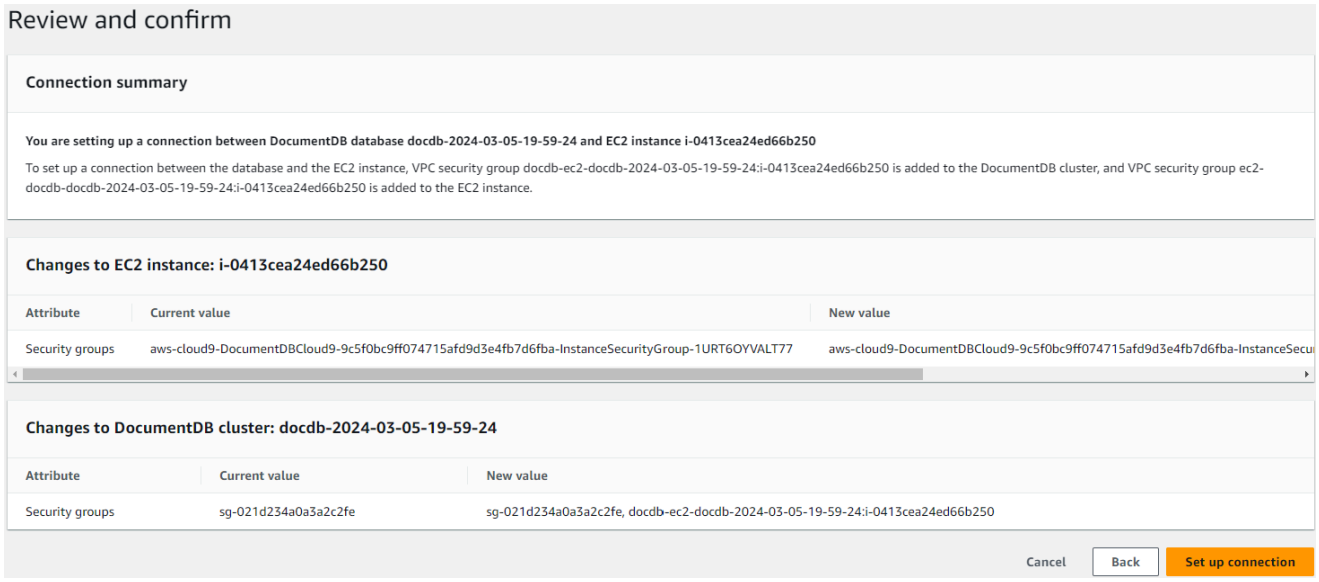
b. En el campo de EC2 instancia, elija la EC2 instancia que desee conectar a su clúster.



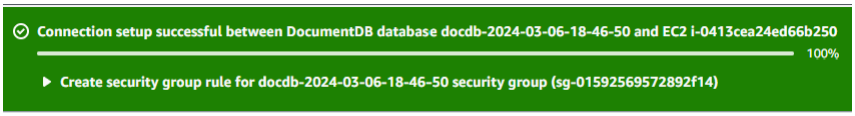
c. Elija Continuar.

Aparece el cuadro de diálogo Revisar y confirmar.

d. Asegúrese de que los cambios sean correctos. A continuación, elija Configurar la conexión.



Si la operación se lleva a cabo correctamente, aparecerá la siguiente verificación:



Descripción general de la conectividad automática con una instancia EC2

Al configurar una conexión entre una EC2 instancia y una base de datos de Amazon DocumentDB, Amazon DocumentDB configura automáticamente el grupo de seguridad de VPC para su instancia EC2 y para su base de datos de Amazon DocumentDB.

Los siguientes son requisitos para conectar una EC2 instancia a una base de datos de Amazon DocumentDB:

- La EC2 instancia debe estar en la misma VPC que la base de datos de Amazon DocumentDB.

  Si no existe ninguna EC2 instancia en la misma VPC, la consola proporciona un enlace para crear una.
- El usuario que configura la conectividad debe tener permisos para realizar las siguientes EC2 operaciones de Amazon:
  - `ec2:AuthorizeSecurityGroupEgress`
  - `ec2:AuthorizeSecurityGroupIngress`
  - `ec2:CreateSecurityGroup`
  - `ec2:DescribeInstances`

- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeSecurityGroups`
- `ec2:ModifyNetworkInterfaceAttribute`
- `ec2:RevokeSecurityGroupEgress`

Si la instancia de base de datos y la EC2 instancia se encuentran en zonas de disponibilidad diferentes, es posible que su cuenta incurra en costes por zonas de disponibilidad cruzada.

Al configurar una conexión a una EC2 instancia, Amazon DocumentDB actúa de acuerdo con la configuración actual de los grupos de seguridad asociados a la base de datos y la instancia de Amazon DocumentDB, tal EC2 y como se describe en la siguiente tabla:

Configuración actual del grupo de seguridad de Amazon DocumentDB	Configuración actual del grupo EC2 de seguridad	Acción de Amazon DocumentDB
Hay uno o más grupos de seguridad asociados a la base de datos de Amazon DocumentDB con un nombre que coincide con el patrón `DocumentDB-ec2-n` . No se ha modificado ningún grupo de seguridad que coincida con el patrón. Este grupo de seguridad solo tiene una regla de entrada con el grupo de seguridad de VPC de EC2 la instancia como origen.	Hay uno o más grupos de seguridad asociados a la EC2 instancia con un nombre que coincide con el patrón `DocumentDB-ec2-n` (donde n es un número). No se ha modificado ningún grupo de seguridad que coincida con el patrón. Este grupo de seguridad solo tiene una regla de salida con el grupo de seguridad de VPC de la base de datos de Amazon DocumentDB como origen.	Amazon DocumentDB no lleva a cabo ninguna acción. Ya se configuró automáticamente una conexión entre la EC2 instancia y la base de datos Amazon DocumentDB. Como ya existe una conexión entre la EC2 instancia y la base de datos Amazon DocumentDB, los grupos de seguridad no se modifican.
Se aplica alguna de las siguientes condiciones: • No hay ningún grupo de seguridad asociado a la base de datos de Amazon	Se aplica alguna de las siguientes condiciones: • No hay ningún grupo de seguridad asociado a la EC2 instancia con un	Acción de Amazon DocumentDB: creación de nuevos grupos de seguridad

Configuración actual del grupo de seguridad de Amazon DocumentDB	Configuración actual del grupo EC2 de seguridad	Acción de Amazon DocumentDB
DocumentDB con un nombre que coincide con el patrón `DocumentDB-ec2-n`. • Hay uno o más grupos de seguridad asociados a Amazon DocumentDB con un nombre que coincide con el patrón `DocumentDB-ec2-n` . Sin embargo, Amazon DocumentDB no puede usar ninguno de estos grupos de seguridad para la conexión con la EC2 instancia. Amazon DocumentDB no puede usar un grupo de seguridad que no tenga una regla de entrada con el grupo de seguridad de VPC de la EC2 instancia como origen. Amazon DocumentDB tampoco puede usar un grupo de seguridad que se haya modificado. Los ejemplos de modificaciones incluyen agregar una regla o cambiar el puerto de una regla existente.	nombre que coincida con el patrón. `ec2-DocumentDB-n` • Hay uno o más grupos de seguridad asociados a la EC2 instancia con un nombre que coincide con el patrón`ec2-DocumentDB-n`. Sin embargo, Amazon DocumentDB no puede usar ninguno de estos grupos de seguridad para la conexión con la base de datos de Amazon DocumentDB. Amazon DocumentDB no puede usar un grupo de seguridad que no tenga una regla de salida con el grupo de seguridad de la VPC de la base de datos de Amazon DocumentDB como origen. Amazon DocumentDB tampoco puede usar un grupo de seguridad que se haya modificado.	

Configuración actual del grupo de seguridad de Amazon DocumentDB	Configuración actual del grupo EC2 de seguridad	Acción de Amazon DocumentDB
Hay uno o más grupos de seguridad asociados a la base de datos de Amazon DocumentDB con un nombre que coincide con el patrón `DocumentDB-ec2-n` . No se ha modificado ningún grupo de seguridad que coincida con el patrón. Este grupo de seguridad solo tiene una regla de entrada con el grupo de seguridad de VPC de EC2 la instancia como origen.	Hay uno o más grupos de seguridad asociados a la EC2 instancia con un nombre que coincide con el patrón. `ec2-DocumentDB-n` Sin embargo, Amazon DocumentDB no puede usar ninguno de estos grupos de seguridad para la conexión con la base de datos de Amazon DocumentDB. Amazon DocumentDB no puede usar un grupo de seguridad que no tenga una regla de salida con el grupo de seguridad de la VPC de la base de datos de Amazon DocumentDB como origen. Amazon DocumentDB tampoco puede usar un grupo de seguridad que se haya modificado.	Acción de Amazon DocumentDB: creación de nuevos grupos de seguridad

Configuración actual del grupo de seguridad de Amazon DocumentDB	Configuración actual del grupo EC2 de seguridad	Acción de Amazon DocumentDB
Hay uno o más grupos de seguridad asociados a la base de datos de Amazon DocumentDB con un nombre que coincide con el patrón `DocumentDB-ec2-n` . No se ha modificado ningún grupo de seguridad que coincida con el patrón. Este grupo de seguridad solo tiene una regla de entrada con el grupo de seguridad de VPC de EC2 la instancia como origen.	Existe un grupo EC2 de seguridad válido para la conexión, pero no está asociado a la EC2 instancia . Este grupo de seguridad tiene un nombre que coincide con el patrón `DocumentDB-ec2-n`. No se ha modificado. Solo tiene una regla de salida con el grupo de seguridad de VPC de la base de datos de Amazon DocumentDB como origen.	Acción de Amazon DocumentDB: asociar EC2 grupo de seguridad

Configuración actual del grupo de seguridad de Amazon DocumentDB	Configuración actual del grupo EC2 de seguridad	Acción de Amazon DocumentDB
Se aplica alguna de las siguientes condiciones: • No hay ningún grupo de seguridad asociado a la base de datos de Amazon DocumentDB con un nombre que coincide con el patrón `DocumentDB-ec2-n`. • Hay uno o más grupos de seguridad asociados a la base de datos de Amazon DocumentDB con un nombre que coincide con el patrón `DocumentDB-ec2-n` . Sin embargo, Amazon DocumentDB no puede usar ninguno de estos grupos de seguridad para la conexión con la EC2 instancia. Amazon DocumentDB no puede usar un grupo de seguridad que no tenga una regla de entrada con el grupo de seguridad de VPC de la EC2 instancia como origen. Amazon DocumentDB tampoco puede usar un grupo de seguridad modificado.	Hay uno o más grupos de seguridad asociados a la EC2 instancia con un nombre que coincide con el patrón `DocumentDB-ec2-n` No se ha modificado ningún grupo de seguridad que coincida con el patrón. Este grupo de seguridad solo tiene una regla de salida con el grupo de seguridad de VPC de la base de datos de Amazon DocumentDB como origen.	Acción de Amazon DocumentDB: creación de nuevos grupos de seguridad

Acción de Amazon DocumentDB: creación de nuevos grupos de seguridad

Amazon DocumentDB lleva a cabo las siguientes acciones:

- Crea un nuevo grupo de seguridad que coincide con el patrón `DocumentDB-ec2-n`. Este grupo de seguridad tiene una regla de entrada con el grupo de seguridad de VPC de EC2 la instancia como origen. Este grupo de seguridad está asociado a la base de datos Amazon DocumentDB y permite que la EC2 instancia acceda a la base de datos Amazon DocumentDB.
- Crea un nuevo grupo de seguridad que coincide con el patrón `ec2-DocumentDB-n`. Este grupo de seguridad tiene una regla de salida con el grupo de seguridad de VPC de la base de datos de Amazon DocumentDB como origen. Este grupo de seguridad está asociado a la EC2 instancia y permite que la EC2 instancia envíe tráfico a la base de datos Amazon DocumentDB.

Acción de Amazon DocumentDB: asociar EC2 grupo de seguridad

Amazon DocumentDB asocia el grupo de EC2 seguridad válido y existente a la EC2 instancia. Este grupo de seguridad permite que la EC2 instancia envíe tráfico a la base de datos Amazon DocumentDB.

Visualización de los recursos de computación conectados

Puede utilizarla Consola de administración de AWS para ver los recursos informáticos que están conectados a una base de datos de Amazon DocumentDB. Los recursos que se muestran incluyen conexiones de recursos informáticos que se configuraron automáticamente. Puede definir la conectividad con los recursos informáticos de manera automática de las siguientes maneras:

- Puede seleccionar el recurso informático al crear la base de datos. Para obtener más información, consulte Creación de un clúster de Amazon DocumentDB y Creación de un clúster de base de datos Multi-AZ.
- Puede configurar la conectividad entre una base de datos existente y un recurso informático. Para obtener más información, consulte Connect Amazon EC2 automáticamente.

Los recursos informáticos de la lista no incluyen los que se conectaron a la base de datos manualmente. Por ejemplo, puede permitir que un recurso informático acceda a una base de datos manualmente añadiendo una regla al grupo de seguridad de la VPC asociado a la base de datos.

Para que un recurso informático coincida, se deben cumplir las siguientes condiciones:

- El nombre del grupo de seguridad asociado al recurso de computación coincide con el patrón `ec2-DocumentDB-n` (donde n es un número).
- El grupo de seguridad asociado al recurso de computación tiene una regla de salida con el rango de puertos establecido en el puerto utilizado por la base de datos de Amazon DocumentDB.
- El grupo de seguridad asociado al recurso de computación tiene una regla de salida en la que el origen está establecido en un grupo de seguridad asociado a la base de datos de Amazon DocumentDB.
- El nombre del grupo de seguridad asociado a la base de datos de Amazon DocumentDB coincide con el patrón `DocumentDB-ec2-n` (donde n es un número).
- El grupo de seguridad asociado a la base de datos de Amazon DocumentDB tiene una regla de entrada con el rango de puertos establecido en el puerto utilizado por la base de datos de Amazon DocumentDB.
- El grupo de seguridad asociado a la base de datos de Amazon DocumentDB tiene una regla de entrada con el origen establecido en un grupo de seguridad asociado al recurso de computación.

Visualización de los recursos de computación que están conectados a una base de datos de Amazon DocumentDB

1. Inicie sesión en y abra la Consola de administración de AWS consola de Amazon DocumentDB en https://console.aws.amazon.com /docdb.
2. En el panel de navegación, elija Bases de datos y, luego, el nombre de la instancia de base de datos de Amazon DocumentDB.
3. En la pestaña Conectividad y seguridad, consulte los recursos de computación en la sección Recursos de computación conectados.

Connect Amazon EC2 manualmente

Temas

- Paso 1: Crear una EC2 instancia de Amazon
- Paso 2: crear un grupo de seguridad
- Paso 3: crear un clúster de Amazon DocumentDB
- Paso 4: Conéctate a tu EC2 instancia de Amazon
- Paso 5: instalación del intérprete de comandos de MongoDB
- Paso 6: administrar TLS de Amazon DocumentDB

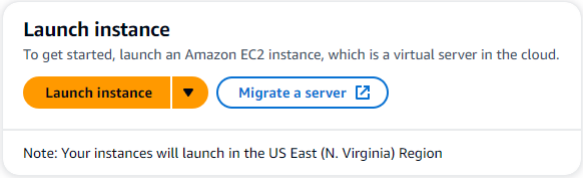
- Paso 7: conectarse a su clúster de Amazon DocumentDB
- Paso 8: insertar y consultar datos
- Paso 9: explorar

En los siguientes pasos se presupone que ha completado los pasos que se detallan en el tema Requisitos previos.

Paso 1: Crear una EC2 instancia de Amazon

En este paso, creará una EC2 instancia de Amazon en la misma región y Amazon VPC que utilizará más adelante para aprovisionar el clúster de Amazon DocumentDB.

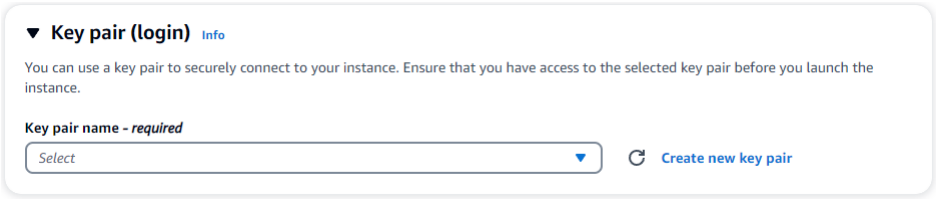
1. En la EC2 consola de Amazon, selecciona Launch instance.



2. Ingrese un nombre o identificador en el campo Nombre ubicado en la sección Nombres y etiquetas.
3. En la lista desplegable Imagen de máquina de Amazon (AMI), busque la AMI de Amazon Linux 2 y selecciónela.



4. Busque y seleccione t3.micro en la lista desplegable de Tipo de instancia.
5. En la sección Par de claves (inicio de sesión), ingrese el identificador de un par de claves existente o elija Crear un par de claves nuevo.

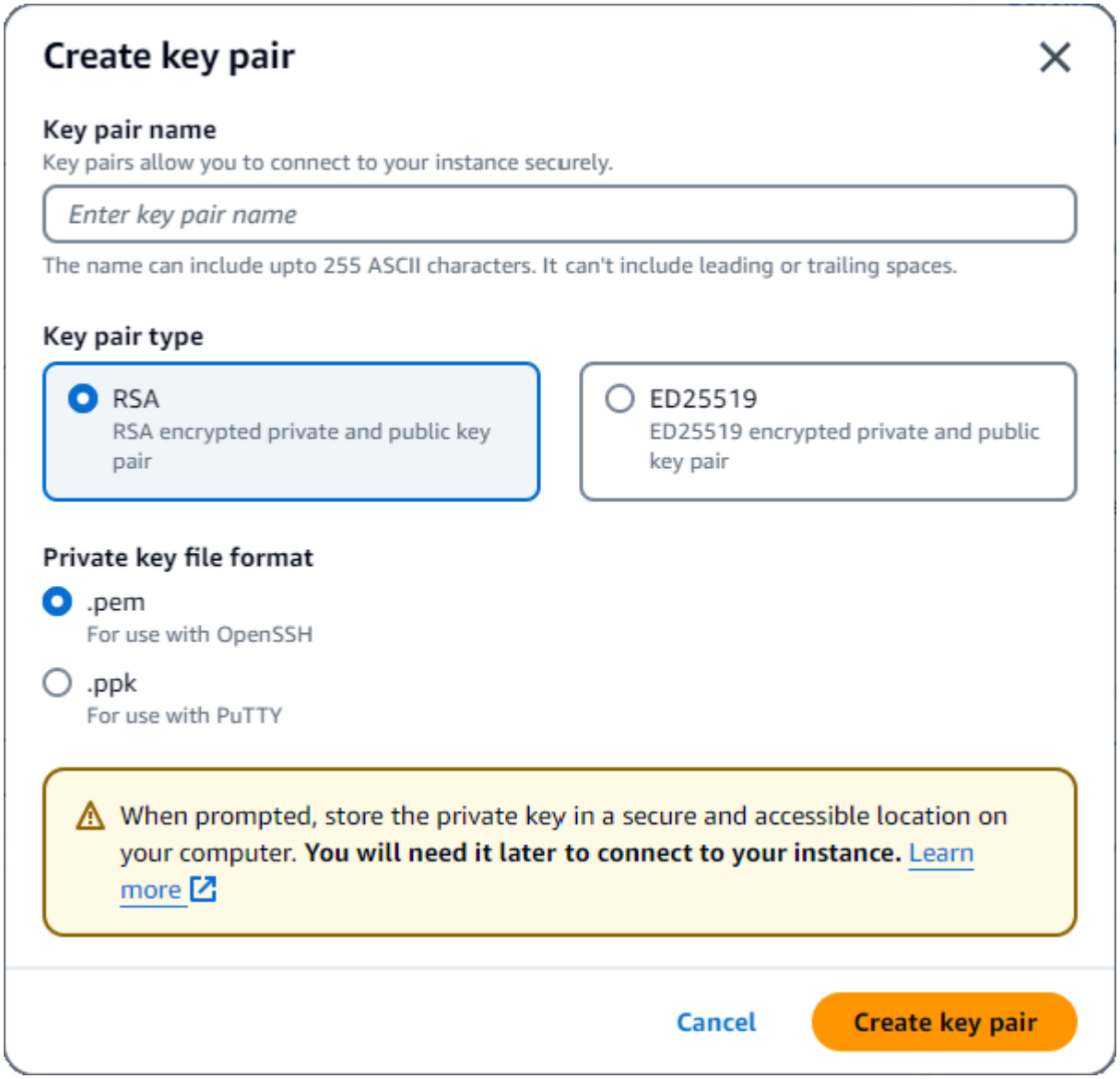


Debes proporcionar un EC2 key pair de Amazon.

- Si tienes un par de EC2 claves de Amazon:

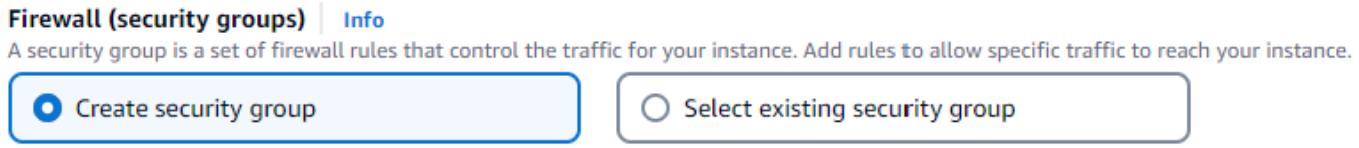
1. Seleccione un par de claves, elija su par de claves de la lista.
2. Debes tener ya disponible el archivo de clave privada (archivo.pem o.ppk) para iniciar sesión en tu instancia de Amazon. EC2

- Si no tienes un par de EC2 claves de Amazon:
  1. Seleccione Crear un par de claves nuevo y aparecerá el cuadro de diálogo Crear par de claves.
  2. Escriba un nombre en el campo Nombre del par de claves.
  3. Seleccione el Tipo de par de claves y el Formato de archivo de clave privada.
  4. Elija Crear par de claves.



> **Note**
>
> Por motivos de seguridad, te recomendamos encarecidamente que utilices un par de claves para la conectividad SSH y a Internet con tu instancia. EC2

6. En la sección Configuración de red, en Firewall (grupos de seguridad), elija Crear grupo de seguridad o Seleccionar grupo de seguridad existente.



   Si opta por seleccionar un grupo de seguridad existente, seleccione uno en la lista desplegable de Grupos de seguridad comunes.

   Si ha optado por crear un grupo de seguridad nuevo, haga lo siguiente:

   a. Comprueba todas las reglas de tráfico que se apliquen a tu conectividad. EC2

   b. En el campo IP, elija Mi IP o seleccione Personalizado para elegir entre una lista de bloques de CIDR, listas de prefijos o grupos de seguridad. No recomendamos Anywhere como opción, a menos que la EC2 instancia esté en una red aislada, ya que permite el acceso a la EC2 instancia desde cualquier dirección IP.

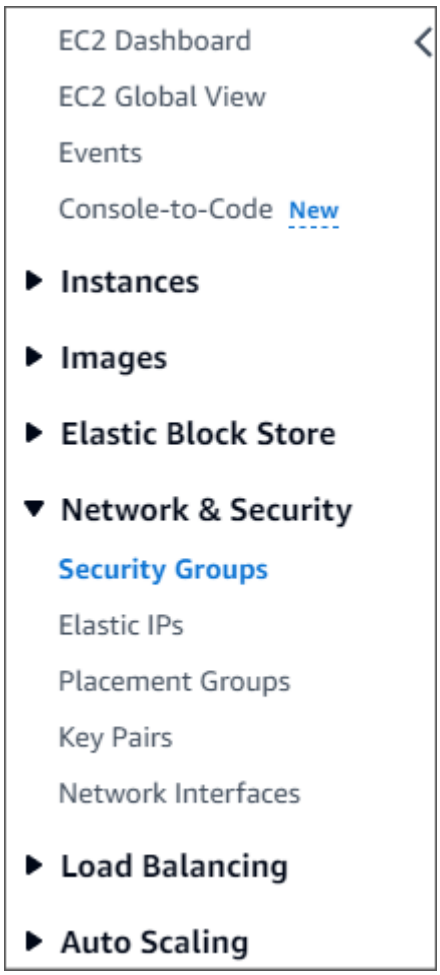


7. En la sección Resumen, revisa la EC2 configuración y, si es correcta, selecciona Launch instance.

Paso 2: crear un grupo de seguridad

Ahora creará un nuevo grupo de seguridad en su Amazon VPC predeterminada. El grupo de seguridad `demoDocDB` le permite conectarse a su clúster de Amazon DocumentDB en el puerto 27017 (el puerto predeterminado de Amazon DocumentDB) desde su instancia de Amazon. EC2

1. En Amazon EC2 Management Console, en Red y seguridad, selecciona Grupos de seguridad.



2. Elija Creación de grupo de seguridad.



3. En la sección Detalles básicos:

   a. En Nombre del grupo de seguridad, introduzca `demoDocDB`.

   b. En Descripción, escriba una descripción.

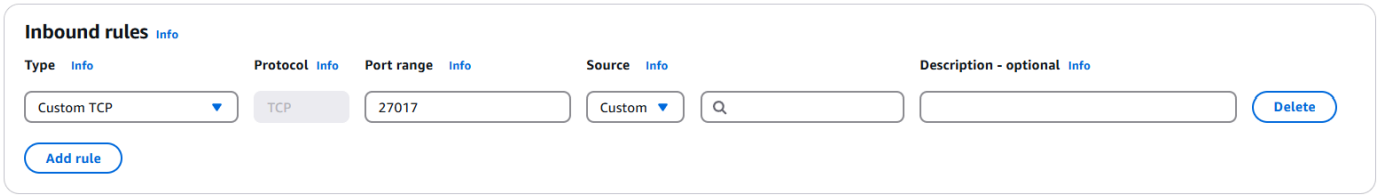
   c. En VPC, acepte el uso de la VPC predeterminada.

4. En la sección Inbound rules (Reglas de entrada), elija Add rule (agregar regla).

   a. En Tipo, elija Regla TCP personalizada (predeterminada).

   b. En Rango de puertos, introduzca `27017`.

   c. En Source (Origen), seleccione Custom (Personalizado). En el campo contiguo, busque el grupo de seguridad que acaba de crear en el paso 1. Puede que tengas que actualizar tu navegador para que la EC2 consola de Amazon rellene automáticamente el nombre de la fuente.



5. Acepte todos los demás valores predeterminados y elija Crear grupo de seguridad.



Paso 3: crear un clúster de Amazon DocumentDB

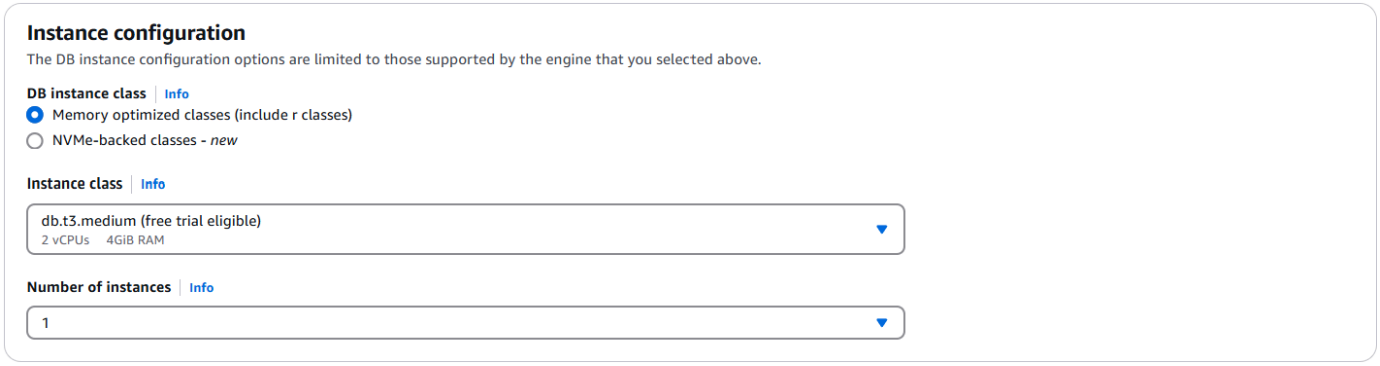
Mientras se aprovisiona la EC2 instancia de Amazon, creará su clúster de Amazon DocumentDB.

1. Navegue hasta la consola de Amazon DocumentDB y elija Clústeres en el panel de navegación.
2. Seleccione Crear.
3. Deje la configuración de Tipo de clúster como predeterminada en Clúster basado en instancias.
4. En Configuración del clúster, ingrese un nombre único en Identificador de clúster. Tenga en cuenta que la consola cambiará todos los nombres de los clústeres a minúsculas independientemente de cómo se ingresen.

   Deje Versión del motor con su valor predeterminado de 5.0.0.
5. En Configuración del almacenamiento en clúster, deje la configuración predeterminada de Amazon DocumentDB estándar.
6. En Configuración de instancias:

   - En Clase de instancia de base de datos, elija Clases optimizadas para memoria (incluidas las clases r), que es la opción predeterminada.

     La otra opción de instancia son las clases respaldadas por NVMecomandos. Para obtener más información, consulte Instancias respaldadas por NVMe.
   - En Clase de instancia, elija el tipo de instancia que se adapte a sus necesidades. Para obtener una explicación más detallada de las clases de instancia, consulte Especificaciones de clases de instancias.
   - En Número de instancias, elija el número que mejor refleje sus necesidades. Recuerde que cuanto menor sea el número, menor será el costo y menor será el read/write volumen que puede administrar el clúster.



7. En Conectividad, deje la configuración predeterminada de No conectarse a un recurso de EC2 cómputo.

> **Note**
>
> La conexión a un recurso EC2 informático crea automáticamente grupos de seguridad para la conexión al clúster. Como en el paso anterior creó estos grupos de seguridad manualmente, debe seleccionar No conectarse a un recurso EC2 informático para no crear un segundo conjunto de grupos de seguridad.

8. En la sección Autenticación, ingrese un nombre de usuario para el usuario principal y, a continuación, elija Autoadministrado. Ingrese una contraseña y, a continuación, confírmela.

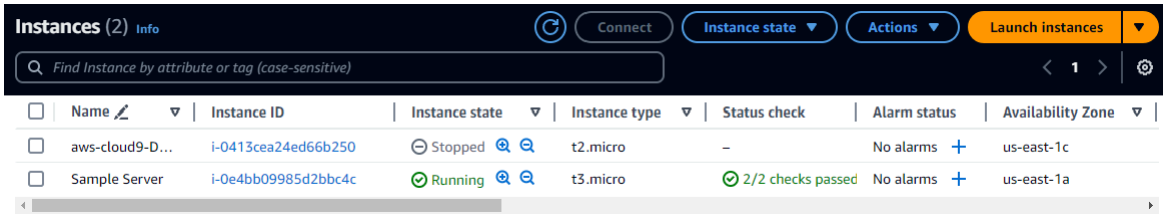
   Si, en su lugar, eligió Administrado en AWS Secrets Manager, consulte Administración de contraseñas con Amazon DocumentDB y AWS Secrets Manager para obtener más información.

9. Elija Create cluster.

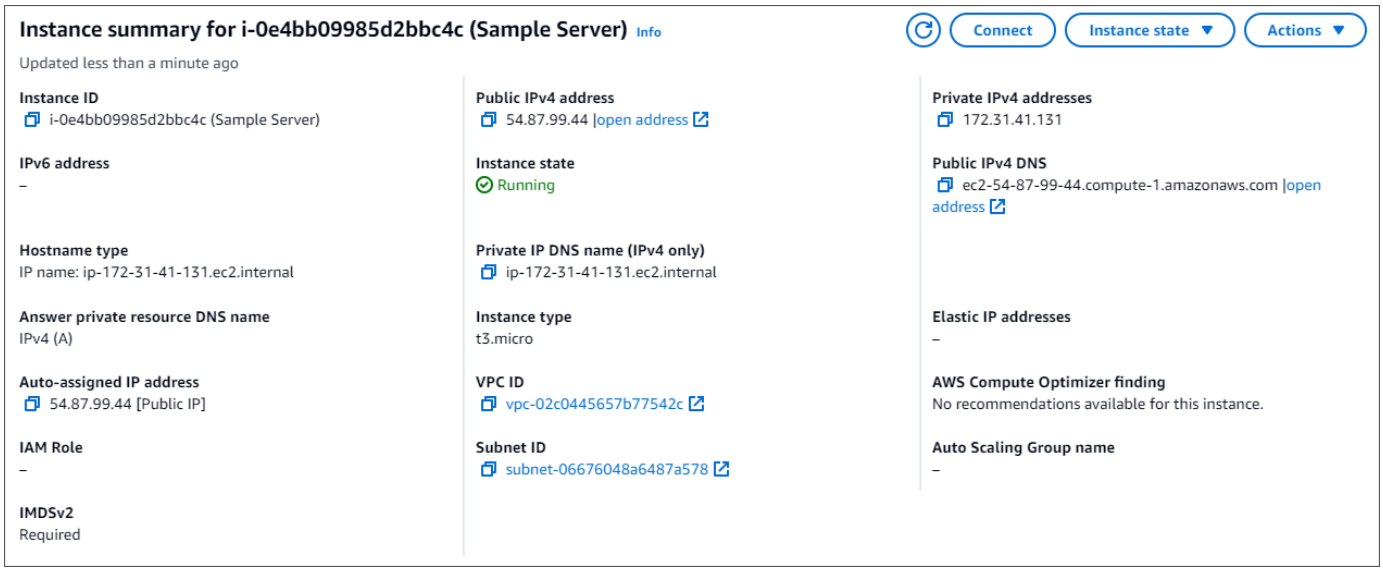
Paso 4: Conéctate a tu EC2 instancia de Amazon

Si te conectas a tu EC2 instancia de Amazon, podrás instalar el shell de MongoDB. La instalación del intérprete de comandos de mongo permite conectarse a su clúster de Amazon DocumentDB y realizar consultas en él. Realice los siguientes pasos:

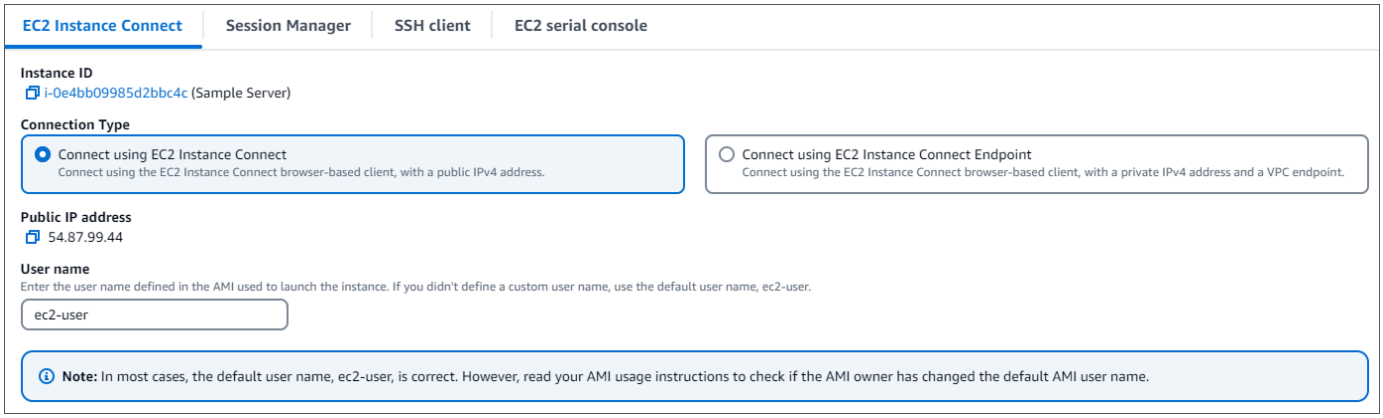
1. En la EC2 consola de Amazon, navega hasta tus instancias y comprueba si la instancia que acabas de crear se está ejecutando. Si es así, haga clic en el ID de la instancia para seleccionar la instancia.



2. Elija Conectar.



3. Existen cuatro opciones con pestañas para su método de conexión: Amazon EC2 Instance Connect, Session Manager, cliente SSH o consola EC2 serie. Debe elegir uno y seguir sus instrucciones. Cuando haya terminado, elija Conectar.



> **Note**
>
> Si su dirección IP ha cambiado después de iniciar este tutorial o si va a volver a su entorno más adelante, debe actualizar la regla de entrada del grupo de seguridad `demoEC2` para habilitar el tráfico entrante desde su nueva dirección de API.

Paso 5: instalación del intérprete de comandos de MongoDB

Ahora puede instalar el intérprete de comandos de MongoDB, que es una utilidad de línea de comandos que se utiliza para conectarse al clúster de Amazon DocumentDB y consultarlo. Actualmente hay dos versiones del intérprete de comandos de MongoDB: la versión más reciente, mongosh, y la versión anterior, el intérprete de comandos de mongo.

> **Important**
>
> Existe una limitación conocida con los controladores de Node.js anteriores a la versión 6.13.1, ya que Amazon DocumentDB no los admite actualmente para la autenticación de identidad de IAM. Los controladores Node.js y las herramientas que utilizan el controlador Node.js (como mongosh) deben actualizarse al controlador Node.js versión 6.13.1 o posterior.

Siga las siguientes instrucciones para instalar el intérprete de comandos de MongoDB en su sistema operativo.

On Amazon Linux

Cómo instalar el intérprete de comandos de MongoDB en Amazon Linux

Si no utiliza IAM y desea utilizar el último intérprete de comandos de MongoDB (mongosh) para conectarse a su clúster de Amazon DocumentDB, siga estos pasos:

1. Cree el archivo de repositorio. En la línea de comandos de la EC2 instancia que creó, ejecute el siguiente comando:

```
echo -e "[mongodb-org-5.0] \nname=MongoDB Repository\nbaseurl=https://
repo.mongodb.org/yum/amazon/2023/mongodb-org/5.0/x86_64/\ngpgcheck=1 \nenabled=1
```

```
 \ngpgkey=https://pgp.mongodb.com/server-5.0.asc" | sudo tee /etc/yum.repos.d/
mongodb-org-5.0.repo
```

2. Cuando esté completo, instale mongosh con una de las siguientes opciones de comando en el símbolo del sistema:

   Opción 1: si eligió el Amazon Linux 2023 predeterminado durante la EC2 configuración de Amazon, introduzca este comando:

   ```
   sudo yum install -y mongodb-mongosh-shared-openssl3
   ```

   Opción 2: si eligió Amazon Linux 2 durante la EC2 configuración de Amazon, introduzca este comando:

   ```
   sudo yum install -y mongodb-mongosh
   ```

Si utiliza IAM, debe utilizar la versión anterior del intérprete de comandos de MongoDB (5.0) para conectarse al clúster de Amazon DocumentDB. Siga estos pasos:

1. Cree el archivo de repositorio. En la línea de comandos de la EC2 instancia que creó, ejecute el siguiente comando:

   ```
   echo -e "[mongodb-org-5.0] \nname=MongoDB Repository\nbaseurl=https://
   repo.mongodb.org/yum/amazon/2023/mongodb-org/5.0/x86_64/\ngpgcheck=1 \nenabled=1
    \ngpgkey=https://pgp.mongodb.com/server-5.0.asc" | sudo tee /etc/yum.repos.d/
   mongodb-org-5.0.repo
   ```

2. Cuando esté completo, instale el intérprete de comandos de MongoDB 5.0 con la siguiente opción de comando en el símbolo del sistema:

   ```
   sudo yum install -y mongodb-org-shell
   ```

On Ubuntu

Cómo instalar mongosh en Ubuntu

1. Importe la clave pública que utilizará el sistema de administración de paquetes.

```
curl -fsSL https://pgp.mongodb.com/server-5.0.asc | sudo gpg --dearmor -o /usr/
share/keyrings/mongodb-server-5.0.gpg
```

2. Cree el archivo de lista `mongodb-org-5.0.list` para MongoDB mediante el comando correspondiente a su versión de Ubuntu.

```
echo "deb [ arch=amd64,arm64 signed-by=/usr/share/keyrings/mongodb-
server-5.0.gpg ] https://repo.mongodb.org/apt/ubuntu focal/mongodb-org/5.0
 multiverse" | sudo tee /etc/apt/sources.list.d/mongodb-org-5.0.list
```

3. Importe y actualice la base de datos del paquete local utilizando el siguiente comando:

```
sudo apt-get update
```

4. Instale mongosh.

```
sudo apt-get install -y mongodb-mongosh
```

Para obtener información sobre cómo instalar las versiones anteriores de MongoDB en un sistema Ubuntu, consulte Install MongoDB Community Edition on Ubuntu.

On other operating systems

Para instalar el intérprete de comandos de mongo en otros sistemas operativos, consulte el tema sobre cómo instalar MongoDB Community Edition en la documentación de MongoDB.

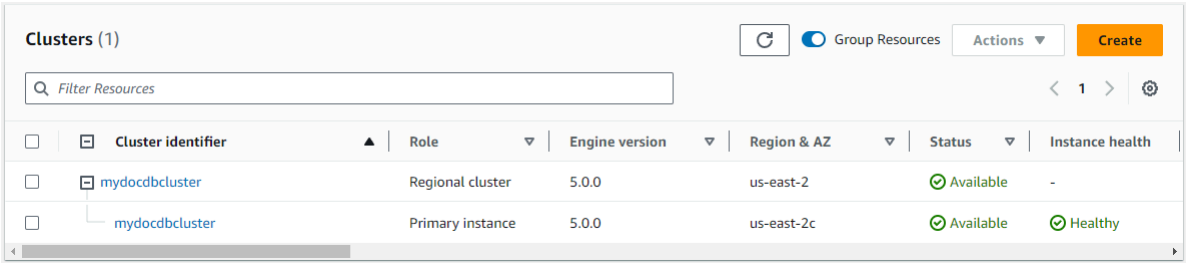
Paso 6: administrar TLS de Amazon DocumentDB

Descargue el certificado CA para Amazon DocumentDB con el siguiente código: `wget https://truststore.pki.rds.amazonaws.com/global/global-bundle.pem`

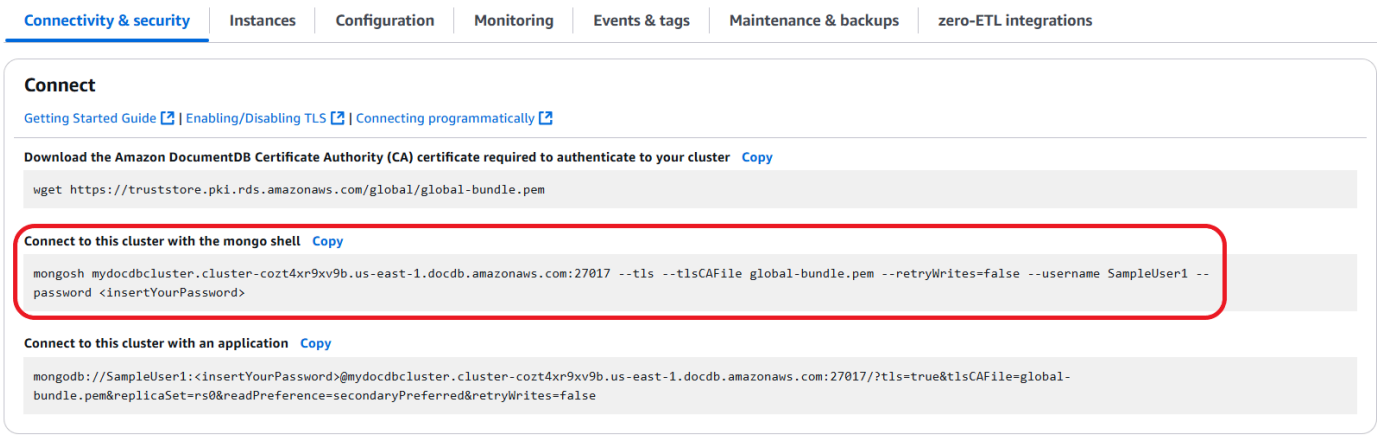
> **Note**
>
> La seguridad de la capa de transporte (TLS) está habilitada de forma predeterminada para todos los clústeres nuevos de Amazon DocumentDB. Para obtener más información, consulte Managing Amazon DocumentDB cluster TLS settings.

Paso 7: conectarse a su clúster de Amazon DocumentDB

1. En la consola de Amazon DocumentDB, en Clústeres, localice su clúster. Haga clic en Identificador del clúster para elegir el clúster que creó.



2. En la pestaña Conectividad y seguridad, busque Conectar a este clúster con el intérprete de comandos de mongo en el cuadro Conectar:



   Copie la cadena de conexión proporcionada y péguela en el terminal.

   Haga los siguientes cambios en ella:

   a. Asegúrese de que tenga el nombre de usuario correcto en la cadena.

   b. Omita `<insertYourPassword>` para que el intérprete de comandos de mongo le pida la contraseña cuando se conecte.

   c. Opcional: si utiliza la autenticación de IAM o utiliza la versión anterior del intérprete de comandos de MongoDB, modifique la cadena de conexión de la siguiente manera:

      ```
      mongo --ssl --host mydocdbcluster.cluster-cozt4xr9xv9b.us-east-1.docdb.amazonaws.com:27017 --sslCAFile global-bundle.pem --username SampleUser1 --password
      ```

Sustituya `mydocdbcluster.cluster-cozt4xr9xv9b.us-east-1` por la misma información de su clúster.

3. Pulse Intro en el terminal. Ahora se le solicitará la contraseña. Introduzca su contraseña.
4. Cuando introduzca la contraseña y pueda ver el mensaje `rs0 [direct: primary] <env-name>>`, significa que se ha conectado correctamente a su clúster de Amazon DocumentDB.

¿Tiene problemas para conectarse? Consulte Solución de problemas de Amazon DocumentDB.

Paso 8: insertar y consultar datos

Ahora que está conectado a su clúster, puede realizar algunas consultas para familiarizarse con el uso de una base de datos de documentos.

1. Para insertar un solo documento, escriba lo siguiente:

```
db.collection.insertOne({"hello":"DocumentDB"})
```

Obtiene el siguiente resultado:

```
{
  acknowledged: true,
  insertedId: ObjectId('673657216bdf6258466b128c')
}
```

2. Puede leer el documento que escribió con el comando `findOne()` (ya que solo devuelve un documento). La siguiente entrada:

```
db.collection.findOne()
```

Obtiene el siguiente resultado:

```
{ "_id" : ObjectId("5e401fe56056fda7321fbd67"), "hello" : "DocumentDB" }
```

3. Para realizar algunas consultas más, plantéese un caso de uso de perfiles de juegos. Primero, inserte algunas entradas en una colección titulada `profiles`. La siguiente entrada:

```
db.profiles.insertMany([{ _id: 1, name: 'Matt', status: 'active', level: 12, score:
 202 },
```

```
      { _id: 2, name: 'Frank', status: 'inactive', level: 2, score: 9 },
      { _id: 3, name: 'Karen', status: 'active', level: 7, score: 87 },
      { _id: 4, name: 'Katie', status: 'active', level: 3, score: 27 }
])
```

Obtiene el siguiente resultado:

```
{ acknowledged: true, insertedIds: { '0': 1, '1': 2, '2': 3, '3': 4 } }
```

4. Utilice el comando `find()` para devolver todos los documentos de la colección de perfiles. La siguiente entrada:

```
db.profiles.find()
```

Obtendrás un resultado que coincidirá con los datos que escribiste en el paso 3.

5. Utilice una consulta para un único documento mediante un filtro. La siguiente entrada:

```
db.profiles.find({name: "Katie"})
```

Obtiene el siguiente resultado:

```
{ "_id" : 4, "name" : "Katie", "status": "active", "level": 3, "score":27}
```

6. Ahora intentemos buscar un perfil y modificarlo con el comando `findAndModify`. Le daremos al usuario Matt 10 puntos adicionales con el siguiente código:

```
db.profiles.findAndModify({
        query: { name: "Matt", status: "active"},
        update: { $inc: { score: 10 } }
    })
```

Se obtiene el siguiente resultado (tenga en cuenta que la puntuación aún no ha aumentado):

```
{
    [{_id : 1, name : 'Matt', status: 'active', level: 12, score: 202}]
```

7. Puede comprobar que su puntuación ha cambiado con la siguiente consulta:

```
db.profiles.find({name: "Matt"})
```

Obtiene el siguiente resultado:

```
{ "_id" : 1, "name" : "Matt", "status" : "active", "level" : 12, "score" : 212 }
```

Paso 9: explorar

¡Enhorabuena! Ha completado correctamente la Guía de inicio rápido para Amazon DocumentDB.

Pasos siguientes Descubra cómo aprovechar al máximo esta potente base de datos con algunas de sus características más populares:

- Administración de Amazon DocumentDB
- Escalado
- Copia de seguridad y restauración

> **Note**
>
> Para ahorrar costos, puede detener el clúster de Amazon DocumentDB para reducir los costos o eliminar el clúster. De forma predeterminada, tras 30 minutos de inactividad, su AWS Cloud9 entorno detendrá la EC2 instancia de Amazon subyacente.

Conexión mediante el controlador JDBC de Amazon DocumentDB

El controlador JDBC para Amazon DocumentDB proporciona una interfaz relacional de SQL para los desarrolladores y permite la conectividad desde herramientas de inteligencia empresarial como Tableau y DbVisualizer.

Para obtener información más detallada, consulte la documentación del controlador JDBC de Amazon DocumentDB en GitHub.

Temas

- Introducción
- Conexión a Amazon DocumentDB desde Tableau Desktop
- Conexión a Amazon DocumentDB desde DbVisualizer
- Generación automática de esquemas JDBC

- Compatibilidad y limitaciones de SQL
- Solución de problemas

Introducción

Paso 1. Creación de un clúster de Amazon DocumentDB

Si no ha creado un clúster de Amazon DocumentDB, cree uno siguiendo las instrucciones de la sección Introducción de la Guía para desarrolladores de Amazon DocumentDB.

> **Note**
>
> Amazon DocumentDB es un servicio exclusivo de nube privada virtual (VPC). Si se conecta desde una máquina local, fuera de la VPC del clúster, necesitará crear una conexión SSH a una instancia de Amazon EC2. En este caso, inicie el clúster siguiendo las instrucciones de Conexión con EC2. Consulte Cómo usar un túnel SSH para conectarse a Amazon DocumentDB para obtener más información sobre los túneles SSH y cuándo podría necesitarlos.

Paso 2. Instalación de JRE o JDK

En función de la aplicación de BI que utilice, es posible que tenga instalada en su ordenador una instalación JRE o JDK de 64 bits, versión 8 o posterior. Puede descargar el Java SE Runtime Environment 8 aquí.

Paso 3. Descarga del controlador JDBC de DocumentDB

Descargue el controlador JDBC de DocumentDB desde aquí. El controlador está empaquetado como un único archivo JAR (por ejemplo, documentdb-jdbc-1.0.0-all.jar).

Paso 4. Cómo usar un túnel SSH para conectarse a Amazon DocumentDB

Los clústeres de Amazon DocumentDB (con compatibilidad con MongoDB) se implementan en una instancia de Amazon Virtual Private Cloud (Amazon VPC). Se puede obtener acceso a ellos directamente mediante instancias de Amazon EC2 u otros servicios de AWS que se implementen en la misma Amazon VPC. Además, es posible obtener acceso a Amazon DocumentDB mediante instancias EC2 u otros servicios de AWS en diferentes VPC de la misma región de AWS u otras regiones a través de la interconexión de VPC.

Puede utilizar la tunelización SSH (también conocida como reenvío de puertos) para acceder a los recursos de Amazon DocumentDB desde fuera de la VPC del clúster. Este será el caso de la mayoría de los usuarios que no ejecuten su aplicación en una máquina virtual de la misma VPC que el clúster de DocumentDB.

Para crear un túnel SSH, necesita una instancia de Amazon EC2 que se ejecute en la misma VPC de Amazon que el clúster de Amazon DocumentDB. Puede usar una instancia EC2 existente en la misma VPC que el clúster o crear una. Si es así, puede configurar un túnel de SSH en el clúster de Amazon DocumentDB `sample-cluster.node.us-east-1.docdb.amazonaws.com` ejecutando el siguiente comando en el equipo local.

```
ssh -i "ec2Access.pem" -L 27017:sample-cluster.node.us-
east-1.docdb.amazonaws.com:27017 ubuntu@ec2-34-229-221-164.compute-1.amazonaws.com -
N
```

La marca -L se utiliza para el reenvío de un puerto local. Este es un requisito previo para conectarse a cualquier herramienta de BI que se ejecute en un cliente externo a su VPC. Una vez realizado el paso anterior, puede pasar a los siguientes con la herramienta de BI que prefiera.

Para obtener más información sobre los túneles SSH, consulte la documentación sobre Uso de un túnel SSH para conectarse a Amazon DocumentDB.

Conexión a Amazon DocumentDB desde Tableau Desktop

Temas

- Adición del controlador JDBC de Amazon DocumentDB
- Conexión a Amazon DocumentDB mediante Tableau - Túnel SSH

Adición del controlador JDBC de Amazon DocumentDB

Para conectar con Amazon DocumentDB desde Tableau Desktop, debe descargar e instalar el controlador JDBC de Amazon DocumentDB y el conector de DocumentDB para Tableau.

1. Descargue el archivo JAR del controlador JDBC de Amazon DocumentDB del repositorio de controladores JDBC de Amazon DocumentDB y cópielo en uno de los siguientes directorios según su sistema operativo:

- Windows - `C:\Program Files\Tableau\Drivers`
- MacOS - `~/Library/Tableau/Drivers`

2. Descargue el conector de DocumentDB para Tableau (un archivo TACO) del sitio web de intercambio de Tableau y cópielo en su directorio Mi repositorio/conectores de Tableau.

   - Windows - `C:\Users\[user]\Documents\My Tableau Repository\Connectors`
   - MacOS - `/Users/[user]/Documents/My Tableau Repository/Connectors`

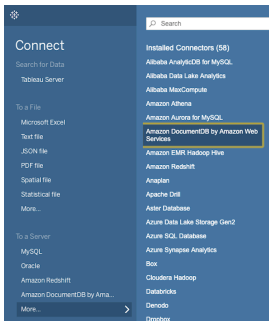
Para obtener información adicional, consulte la documentación de Tableau.

> **Note**
>
> Si utiliza certificados de CA más recientes, asegúrese de actualizar el controlador JDBC a la versión 1.4.5 (disponible en este repositorio de GitHub de AWS).

Conexión a Amazon DocumentDB mediante Tableau - Túnel SSH

Para conectarse a Tableau desde un equipo cliente fuera de la VPC de su clúster de DocumentDB, debe configurar un túnel SSH antes de seguir los pasos que se indican a continuación:

1. Inicie la aplicación Tableau Desktop.
2. Vaya a Conectar > A un servidor > Más.
3. Elija Amazon DocumentDB de Amazon Web Services en Conectores instalados.

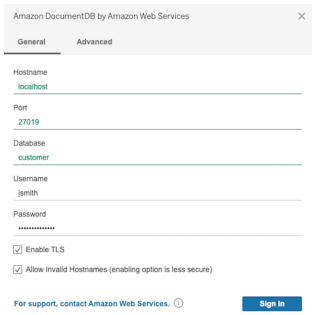


Conexión a Amazon DocumentDB mediante Tableau: túnel SSH externo

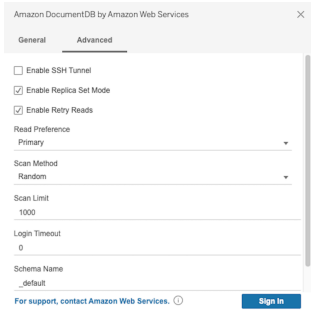
1. Introduzca los parámetros de conexión necesarios: Nombre de host, Puerto, Base de datos, Nombre de usuario y Contraseña. Los parámetros de conexión del ejemplo siguiente son equivalentes a la cadena de conexión JDBC:

   ```
   jdbc:documentdb://localhost:27019/test?
   tls=true&tlsAllowInvalidHostnames=true&scanMethod=random&scanLimit=1000&logir
   ```

   con los parámetros de nombre de usuario y contraseña transferidos por separado en una colección de propiedades. Para obtener más información sobre los parámetros de la cadena de conexión, consulte la documentación de GitHub del controlador JDBC de Amazon DocumentDB.



2. (Opcional) Puede encontrar opciones más avanzadas en la pestaña Avanzado.

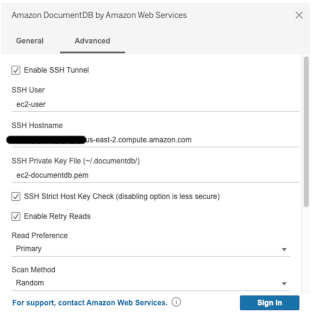


3. Seleccione Iniciar sesión.

Conexión a Amazon DocumentDB mediante Tableau: túnel SSH interno

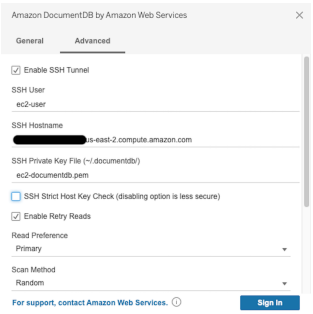
> **Note**
>
> Si prefiere no configurar el túnel SSH mediante un terminal, puede usar la GUI de Tableau para especificar los detalles de su instancia EC2, que el controlador JDBC utilizará de forma inherente para crear un túnel SSH.

1. En la pestaña Avanzado, elija la opción Habilitar el túnel SSH para revisar otras propiedades.



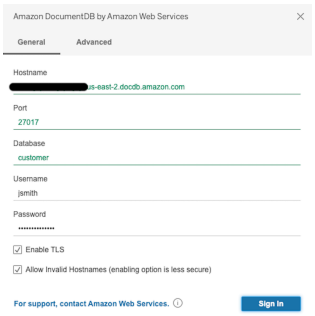
2. Introduzca el Usuario SSH, el Nombre de host SSH y el Archivo de clave privada SSH.
3. (Opcional) Puede deshabilitar la opción de verificación estricta de la clave de host de SSH, que evita la verificación de la clave de host con un archivo de hosts conocido.

> **Note**
>
> Deshabilitar esta opción es menos seguro, ya que puede provocar un ataque de intermediario.



4. Introduzca los parámetros necesarios: Nombre de host, Puerto, Base de datos, Nombre de usuario y Contraseña.

> **Note**
>
> Asegúrese de utilizar el punto de conexión del clúster de DocumentDB y no localhost cuando utilice la opción de túnel SSH interno.



5. Elija Iniciar sesión.

Conexión a Amazon DocumentDB desde DbVisualizer

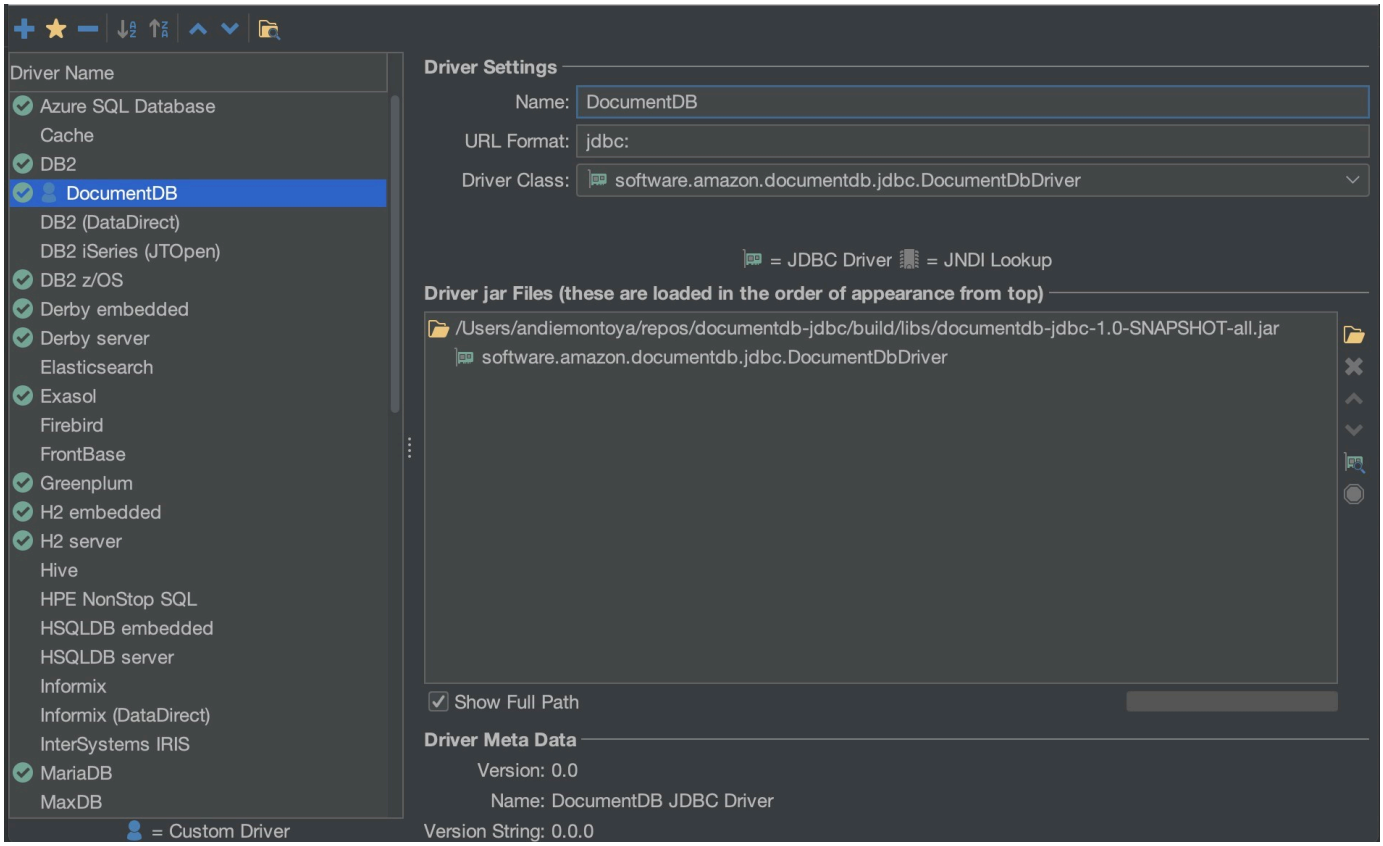
Temas

- Adición del controlador JDBC de Amazon DocumentDB
- Conexión a Amazon DocumentDB mediante DbVisualizer

Adición del controlador JDBC de Amazon DocumentDB

Para conectarse a Amazon DocumentDB desde DbVisualizer, primero debe importar el controlador JDBC de Amazon DocumentDB.

1. Inicie la aplicación DbVisualizer y vaya a la ruta del menú: Herramientas > Administrador de controladores...
2. Elija + (o en el menú, seleccione Controlador > Crear controlador).
3. Establezca Name (Nombre) en `DocumentDB`.
4. Defina el formato de URL en `jdbc:documentdb://<host>[:port]/<database>[?option=value[&option=value[...]]]`
5. Elija el botón de carpeta y luego seleccione el archivo JAR del controlador JDBC de Amazon DocumentDB y luego pulse el botón Abrir.
6. Compruebe que el campo Clase de controlador esté establecido en `software.amazon.documentdb.jdbc.DocumentDbDriver`. La configuración del Administrador de controladores para DocumentDB debe tener el siguiente aspecto.



7. Cierre el cuadro de diálogo. El controlador JDBC de Amazon DocumentDB estará configurado y listo para usarse.

Conexión a Amazon DocumentDB mediante DbVisualizer

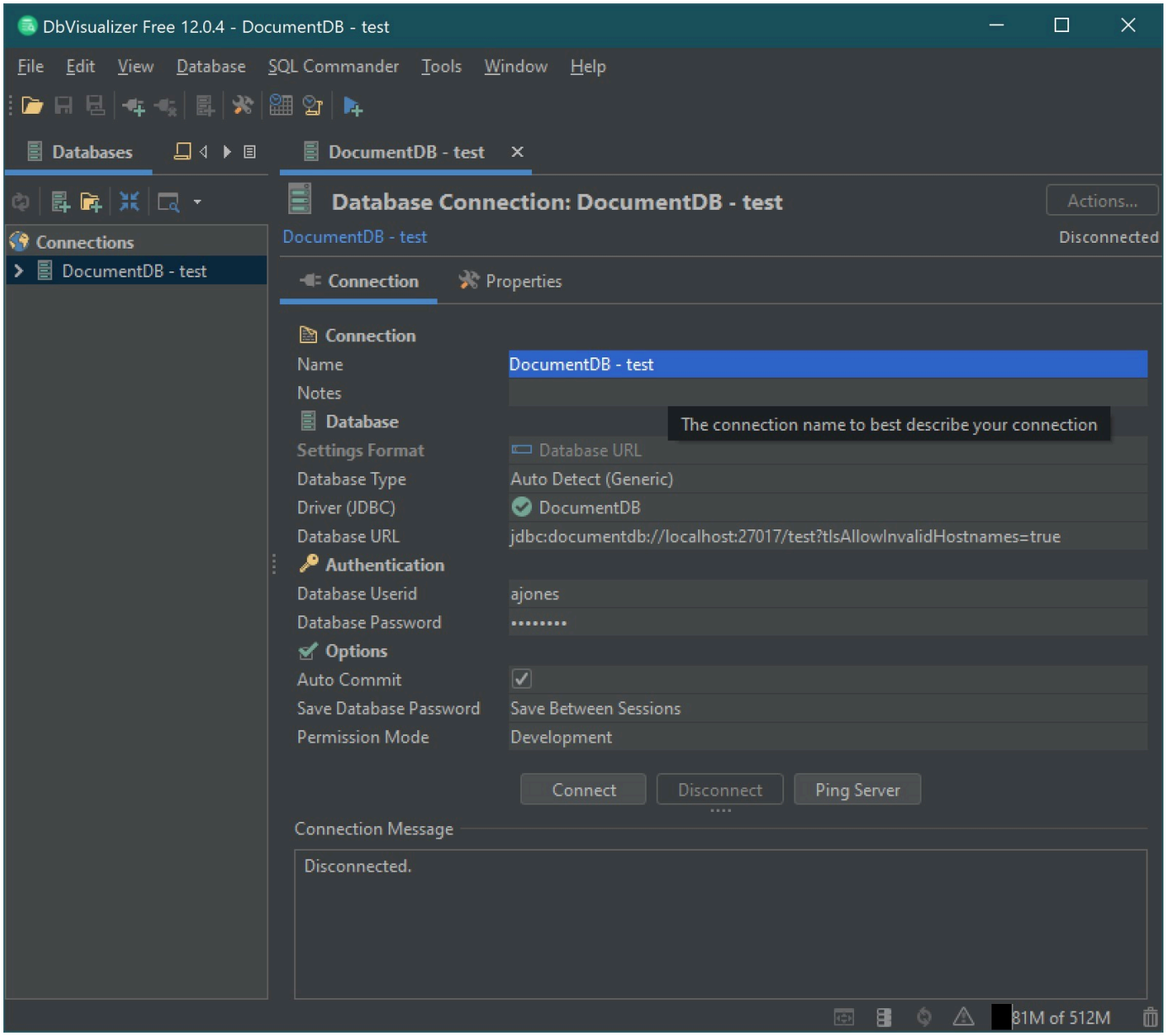
Conexión a Amazon DocumentDB mediante DbVisualizer

1. Si se conecta desde fuera de la VPC del clúster de Amazon DocumentDB, asegúrese de haber configurado un túnel SSH.
2. Seleccione Base de datos > Crear conexión a base de datos en el menú de nivel superior.
3. En el campo Nombre, ingrese un nombre descriptivo.
4. Establezca Controlador (JDBC) en el controlador de DocumentDB que creó en la sección anterior.
5. Establezca la URL de la base de datos en la cadena de conexión JDBC.

   Por ejemplo: .: `jdbc:documentdb://localhost:27017/database?tlsAllowInvalidHostnames=true`
6. Establezca el ID de usuario de la base de datos en su ID de usuario de Amazon DocumentDB.

7. Establezca la contraseña de la base de datos como la contraseña correspondiente al ID de usuario.

   El cuadro de diálogo de conexión a la base de datos debe tener el siguiente aspecto:



8. Elija Connect (Conectar).

Generación automática de esquemas JDBC

Amazon DocumentDB es una base de datos de documentos y, por lo tanto, no tiene el concepto de tablas y esquema. Sin embargo, las herramientas de inteligencia empresarial, como Tableau, esperan que la base de datos a la que se conecta presente un esquema. En concreto, cuando

la conexión del controlador JDBC necesite obtener el esquema de la colección en la base de datos, consultará todas las colecciones de la base de datos. El controlador determinará si ya existe una versión en caché del esquema para esa colección. Si no existe una versión en caché, tomará muestras de la colección de documentos y creará un esquema basado en el siguiente comportamiento.

Temas

- Limitaciones de generación de esquemas
- Opciones del método de análisis
- Tipos de datos de Amazon DocumentDB
- Asignación de campos de documentos escalares
- Manejo de tipos de datos de objetos y matrices

Limitaciones de generación de esquemas

El controlador JDBC de DocumentDB impone un límite de 128 caracteres a la longitud de los identificadores. El generador de esquemas puede truncar la longitud de los identificadores generados (nombres de tablas y nombres de columnas) para garantizar que se ajusten a ese límite.

Opciones del método de análisis

El comportamiento del muestreo se puede modificar mediante la cadena de conexión o las opciones de origen de datos.

- scanMethod=<option>
  - random - (predeterminado): los documentos de muestra se devuelven en orden aleatorio.
  - idForward: los documentos de muestra se devuelven por orden de identificación.
  - idReverse: los documentos de muestra se devuelven por orden inverso de identificación.
  - all (todos): muestra todos los documentos de la colección.
- scanLimit=<n>: el número de documentos que se van a muestrear. El valor debe ser un número entero positivo. El valor predeterminado es 1000. Si ScanMethod está establecido en todos, se omite esta opción.

Tipos de datos de Amazon DocumentDB

El servidor de Amazon DocumentDB admite varios tipos de datos de MongoDB. A continuación se enumeran los tipos de datos compatibles y sus tipos de datos JDBC asociados.

Tipos de datos de MongoDB	Compatible con DocumentDB	Tipo de datos JDBC
Datos Binary	Sí	VARBINARY
Booleano	Sí	BOOLEAN
Doble	Sí	DOBLE
Entero de 32 bits	Sí	INTEGER
Entero de 64 bits	Sí	BIGINT
Cadena	Sí	VARCHAR
ObjectId	Sí	VARCHAR
Date	Sí	TIMESTAMP
Nulo	Sí	VARCHAR
Expresión regular	Sí	VARCHAR
Timestamp	Sí	VARCHAR
MinKey	Sí	VARCHAR
MaxKey	Sí	VARCHAR
Objeto	Sí	tabla virtual
Matriz	Sí	tabla virtual
Decimal128	No	DECIMAL
JavaScript	No	VARCHAR
JavaScript (con alcance)	No	VARCHAR

Tipos de datos de MongoDB	Compatible con DocumentDB	Tipo de datos JDBC
Sin definir	No	VARCHAR
Símbolo	No	VARCHAR
dbPointer (4.0 y versiones posteriores)	No	VARCHAR

Asignación de campos de documentos escalares

Al escanear una muestra de documentos de una colección, el controlador JDBC creará uno o más esquemas para representar las muestras de la colección. En general, un campo escalar del documento se asigna a una columna del esquema de la tabla. Por ejemplo, en una colección denominada team y en un solo documento `{ "_id" : "112233", "name" : "Alastair", "age": 25 }`, esto se asignaría al esquema:

Nombre de la tabla	Nombre de la columna	Tipo de datos	Clave
equipo	id de equipo	VARCHAR	PK
equipo	nombre	VARCHAR	
equipo	edad	INTEGER	

Promoción de conflictos de tipos de datos

Al digitalizar los documentos de muestra, es posible que los tipos de datos de un campo no sean coherentes de un documento a otro. En este caso, el controlador JDBC convertirá el tipo de datos JDBC en un tipo de datos común que se adapte a todos los tipos de datos de los documentos muestreados.

Por ejemplo:

```
{
"_id" : "112233",
"name" : "Alastair", "age" : 25
```

```
}

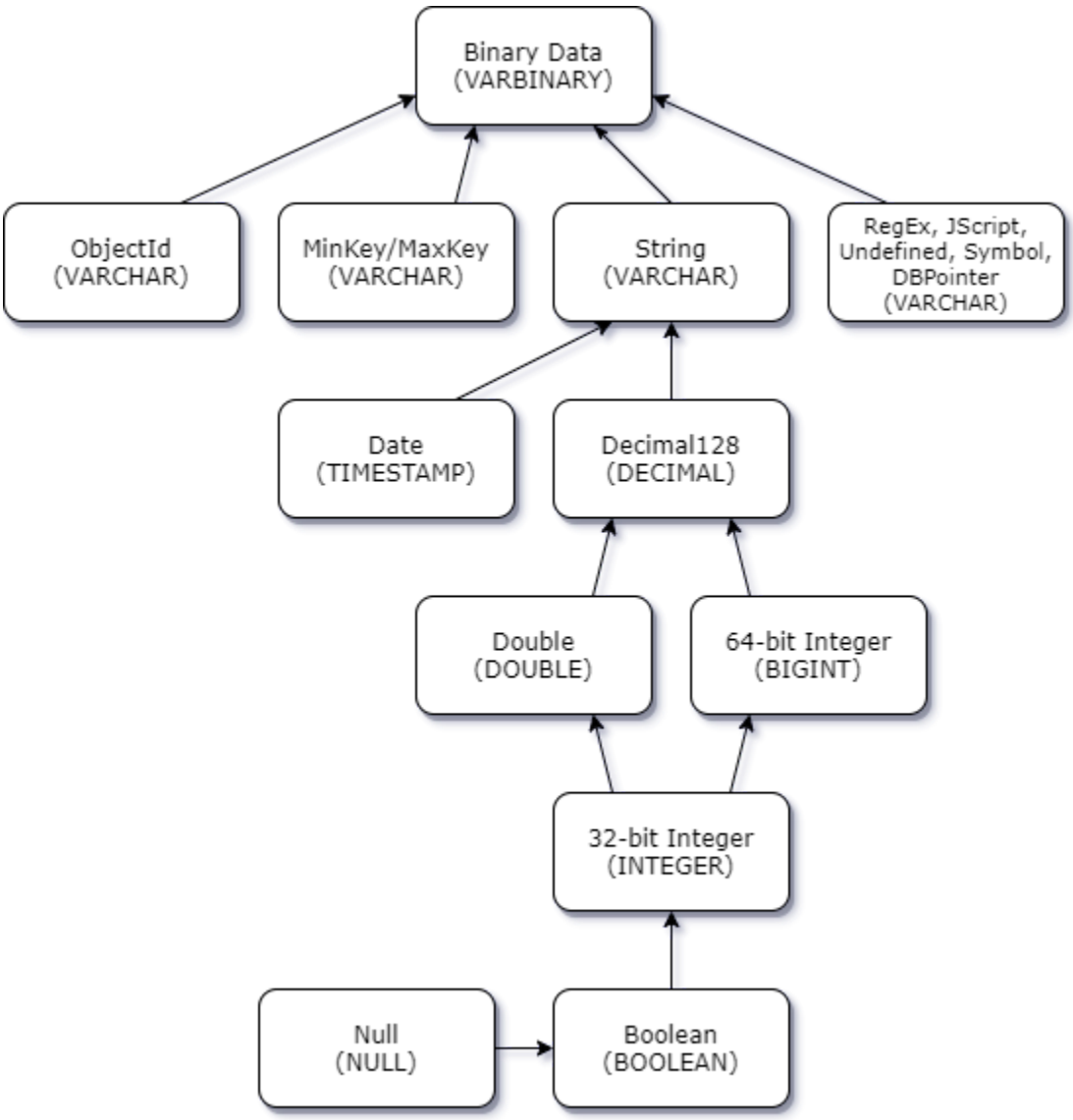
{
"_id" : "112244",
"name" : "Benjamin",
"age" : "32"
}
```

El campo age (edad) es de tipo entero de 32 bits en el primer documento, pero de tipo cadena en el segundo documento. En este caso, el controlador JDBC promoverá el tipo de datos JDBC a VARCHAR para gestionar cualquier tipo de datos cuando los encuentre.

Nombre de la tabla	Nombre de la columna	Tipo de datos	Clave
equipo	id de equipo	VARCHAR	PK
equipo	nombre	VARCHAR	
equipo	edad	VARCHAR	

Promoción de conflictos escalares-escalares

El siguiente diagrama muestra la forma en que se resuelven los conflictos entre tipos de datos escalares-escalares.



Promoción de conflictos de tipo escalar complejo

Al igual que ocurre con los conflictos entre tipos escalares-escalares, un mismo campo en diferentes documentos puede tener tipos de datos conflictivos entre complejos (matriz y objeto) y escalares (enteros, booleanos, etc.). Todos estos conflictos se resuelven (se transfieren) a VARCHAR para esos campos. En este caso, los datos de matriz y objeto se devuelven como representación JSON.

Ejemplo de conflicto entre matriz incrustada y campo de cadena:

```
{
   "_id":"112233",
   "name":"George Jackson",
   "subscriptions":[
```

```
      "Vogue",
      "People",
      "USA Today"
   ]
}
{
   "_id":"112244",
   "name":"Joan Starr",
   "subscriptions":1
}
```

El ejemplo anterior se asigna al esquema de la tabla customer2:

Nombre de la tabla	Nombre de la columna	Tipo de datos	Clave
customer2	Id customer	VARCHAR	PK
customer2	nombre	VARCHAR	
customer2	suscripción	VARCHAR	

y la tabla virtual customer1_subscriptions:

Nombre de la tabla	Nombre de la columna	Tipo de datos	Clave
customer1_subscriptions	Id customer	VARCHAR	PK/FK
customer1_subscriptions	suscriptions_index_lvl0	BIGINT	PK
customer1_subscriptions	valor	VARCHAR	
customer_address	ciudad	VARCHAR	
customer_address	región	VARCHAR	

Nombre de la tabla	Nombre de la columna	Tipo de datos	Clave
customer_address	país	VARCHAR	
customer_address	código	VARCHAR	

Manejo de tipos de datos de objetos y matrices

Hasta ahora, solo hemos descrito cómo se asignan los tipos de datos escalares. Los tipos de datos Object (objeto) y Array (matriz) están (actualmente) asignados a tablas virtuales. El controlador JDBC creará una tabla virtual para representar los campos de objeto o matriz de un documento. El nombre de la tabla virtual asignada concatenará el nombre de la colección original seguido del nombre del campo separado por un carácter de subrayado ("_").

La clave principal de la tabla base ("_id") adopta un nuevo nombre en la nueva tabla virtual y se proporciona como clave externa a la tabla base asociada.

En el caso de los campos de tipo matriz incrustados, las columnas de índice se generan para representar el índice de la matriz en cada nivel de la matriz.

Ejemplo de campo de objeto incrustado

En el caso de los campos de objetos de un documento, el controlador JDBC crea una asignación a una tabla virtual.

```
{
   "Collection: customer",
   "_id":"112233",
   "name":"George Jackson",
   "address":{
      "address1":"123 Avenue Way",
      "address2":"Apt. 5",
      "city":"Hollywood",
      "region":"California",
      "country":"USA",
      "code":"90210"
   }
}
```

El ejemplo anterior se asigna al esquema de la tabla customer (cliente):

Nombre de la tabla	Nombre de la columna	Tipo de datos	Clave
cliente	Id del cliente	VARCHAR	PK
cliente	nombre	VARCHAR	

y la tabla virtual custome_address:

Nombre de la tabla	Nombre de la columna	Tipo de datos	Clave
customer_address	Id del cliente	VARCHAR	PK/FK
customer_address	dirección1	VARCHAR	
customer_address	dirección2	VARCHAR	
customer_address	ciudad	VARCHAR	
customer_address	región	VARCHAR	
customer_address	país	VARCHAR	
customer_address	código	VARCHAR	

Ejemplo de campo de matriz incrustado

En el caso de los campos de objetos de un documento, el controlador JDBC crea una asignación a una tabla virtual.

```
{
   "Collection: customer1",
   "_id":"112233",
   "name":"George Jackson",
   "subscriptions":[
      "Vogue",
      "People",
      "USA Today"
```

```
    ]
}
```

El ejemplo anterior se asigna al esquema de la tabla customer1:

Nombre de la tabla	Nombre de la columna	Tipo de datos	Clave
customer1	Id customer	VARCHAR	PK
customer1	nombre	VARCHAR	

y la tabla virtual customer1_subscriptions:

Nombre de la tabla	Nombre de la columna	Tipo de datos	Clave
customer1_subscriptions	Id customer	VARCHAR	PK/FK
customer1_subscriptions	suscriptions_index_lvl0	BIGINT	PK
customer1_subscriptions	valor	VARCHAR	
customer_address	ciudad	VARCHAR	
customer_address	región	VARCHAR	
customer_address	país	VARCHAR	
customer_address	código	VARCHAR	

Compatibilidad y limitaciones de SQL

El controlador JDBC de Amazon DocumentDB es un controlador de solo lectura que admite un subconjunto de SQL-92 y algunas extensiones comunes. Consulte la documentación sobre las limitaciones de SQL y de JDBC para obtener más información.

Solución de problemas

Si tiene problemas al utilizar el controlador JDBC de Amazon DocumentDB, consulte la Guía de solución de problemas.

Conexión mediante el controlador ODBC de Amazon DocumentDB

El controlador ODBC para Amazon DocumentDB proporciona una interfaz relacional de SQL para los desarrolladores y permite la conectividad desde herramientas de BI como Power BI Desktop y Microsoft Excel.

Para obtener información más detallada, consulte la Documentación del controlador ODBC de Amazon DocumentDB en GitHub.

Temas

- Introducción
- Configuración del controlador ODBC de Amazon DocumentDB en Windows
- Conexión a Amazon DocumentDB desde Microsoft Excel
- Conexión a Amazon DocumentDB desde Power BI Desktop
- Generación automática de esquemas
- Compatibilidad y limitaciones de SQL
- Solución de problemas

Introducción

Paso 1. Creación de clústeres de Amazon DocumentDB

Si todavía no tiene un clúster de Amazon DocumentDB, hay varias formas de empezar.

> **Note**
>
> Amazon DocumentDB es un servicio exclusivo de nube privada virtual (VPC). Si se conecta desde una máquina local externa a la VPC del clúster, necesitará crear una conexión SSH a una instancia de Amazon EC2. En este caso, inicie el clúster siguiendo las instrucciones de Conexión con EC2. Consulte Cómo usar un túnel SSH para conectarse a Amazon DocumentDB para obtener más información sobre los túneles SSH y cuándo podría necesitarlos.

Paso 2. Instalación de JRE o JDK

En función de la aplicación de BI que utilice, puede que necesite instalar en su equipo una versión 8 o posterior de JRE o JDK de 64 bits. Puede descargar el Java SE Runtime Environment 8 aquí.

Paso 3. Descarga del controlador ODBC de Amazon DocumentDB

Descargue el controlador ODBC de Amazon DocumentDB aquí. Elija el instalador adecuado (por ejemplo, documentdb-odbc-1.0.0.msi). Siga la guía de instalación.

Paso 4. Cómo usar un túnel SSH para conectarse a Amazon DocumentDB

Los clústeres de Amazon DocumentDB se implementan dentro de una Amazon Virtual Private Cloud (Amazon VPC). Se puede obtener acceso a ellos directamente mediante instancias de Amazon EC2 u otros servicios de AWS que se implementen en la misma Amazon VPC. Además, es posible obtener acceso a Amazon DocumentDB mediante instancias de Amazon EC2 u otros servicios de AWS en diferentes VPC de la misma región de AWS u otras regiones a través de la interconexión de VPC.

Sin embargo, supongamos que su caso de uso requiere que usted o su aplicación tengan acceso a los recursos de Amazon DocumentDB desde fuera de la VPC del clúster. Este será el caso de la mayoría de los usuarios que no ejecuten su aplicación en una máquina virtual de la misma VPC que el clúster de Amazon DocumentDB. Si se conecta desde fuera de la VPC, puede utilizar la información sobre los túneles SSH (también conocida como reenvío de puertos) para acceder a los recursos de Amazon DocumentDB.

Para crear un túnel SSH, necesita una instancia de Amazon EC2 que se ejecute en la misma VPC de Amazon que el clúster de Amazon DocumentDB. Puede usar una instancia EC2 existente en la misma VPC que el clúster o crear una. Si es así, puede configurar un túnel de SSH en el clúster de Amazon DocumentDB `sample-cluster.node.us-east-1.docdb.amazonaws.com` ejecutando el siguiente comando en su equipo local:

```
ssh -i "ec2Access.pem" -L 27017:sample-cluster.node.us-
east-1.docdb.amazonaws.com:27017 ubuntu@ec2-34-229-221-164.compute-1.amazonaws.com -
N
```

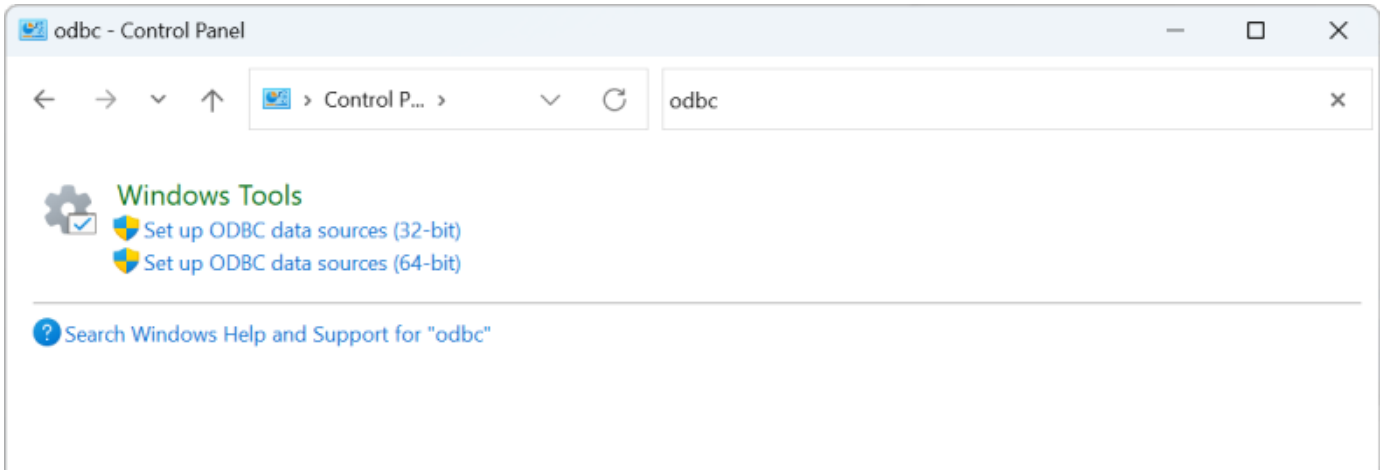
La marca `-L` se utiliza para el reenvío de un puerto local. Este es un requisito previo para conectarse a cualquier herramienta de BI que se ejecute en un cliente externo a su VPC. Una vez realizado el paso anterior, puede pasar a los siguientes con la herramienta de BI que prefiera.

Para obtener más información sobre los túneles SSH, consulte la documentación sobre Cómo usar un túnel SSH para conectarse a Amazon DocumentDB.

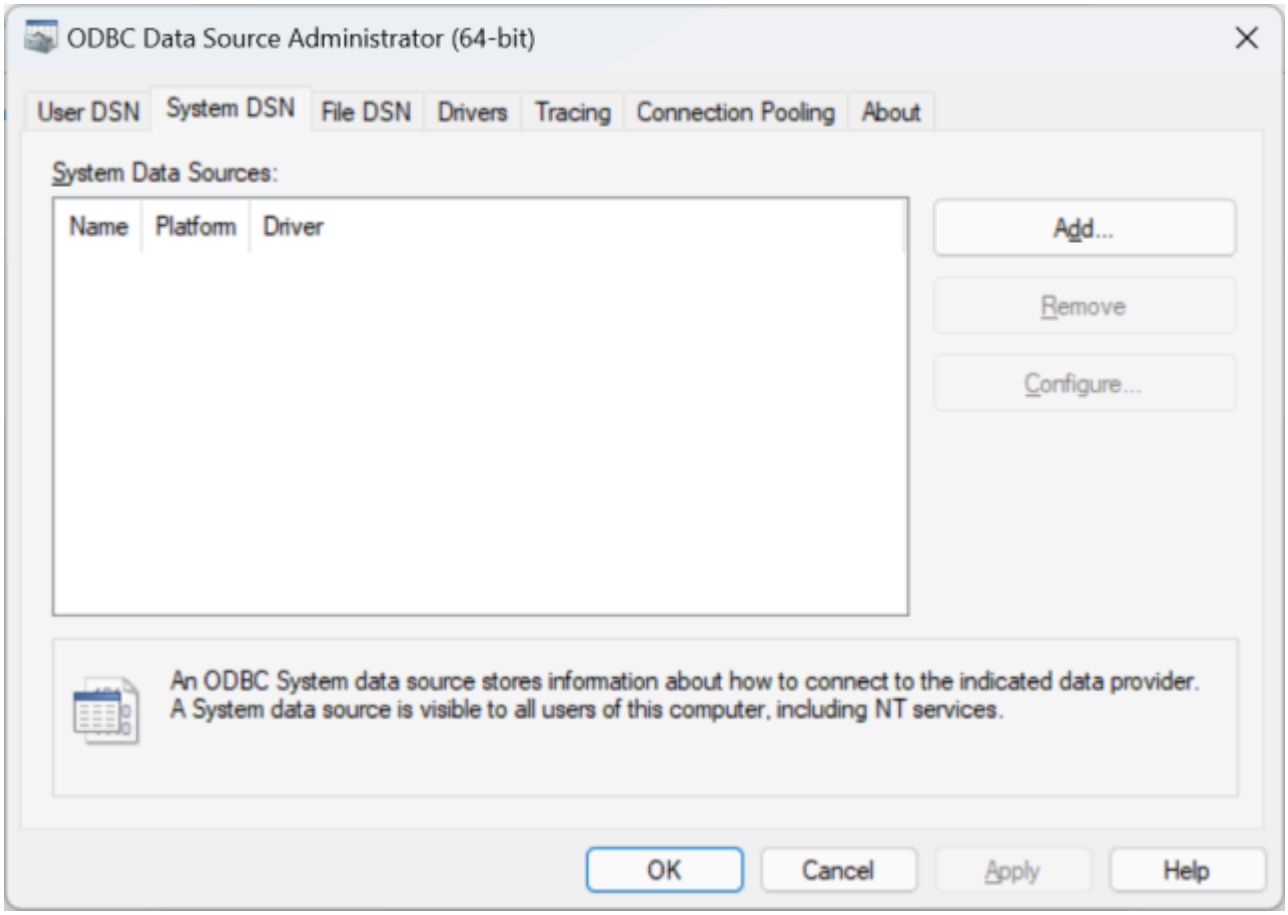
Configuración del controlador ODBC de Amazon DocumentDB en Windows

Utilice el siguiente procedimiento para configurar el controlador ODBC de Amazon DocumentDB en Windows:

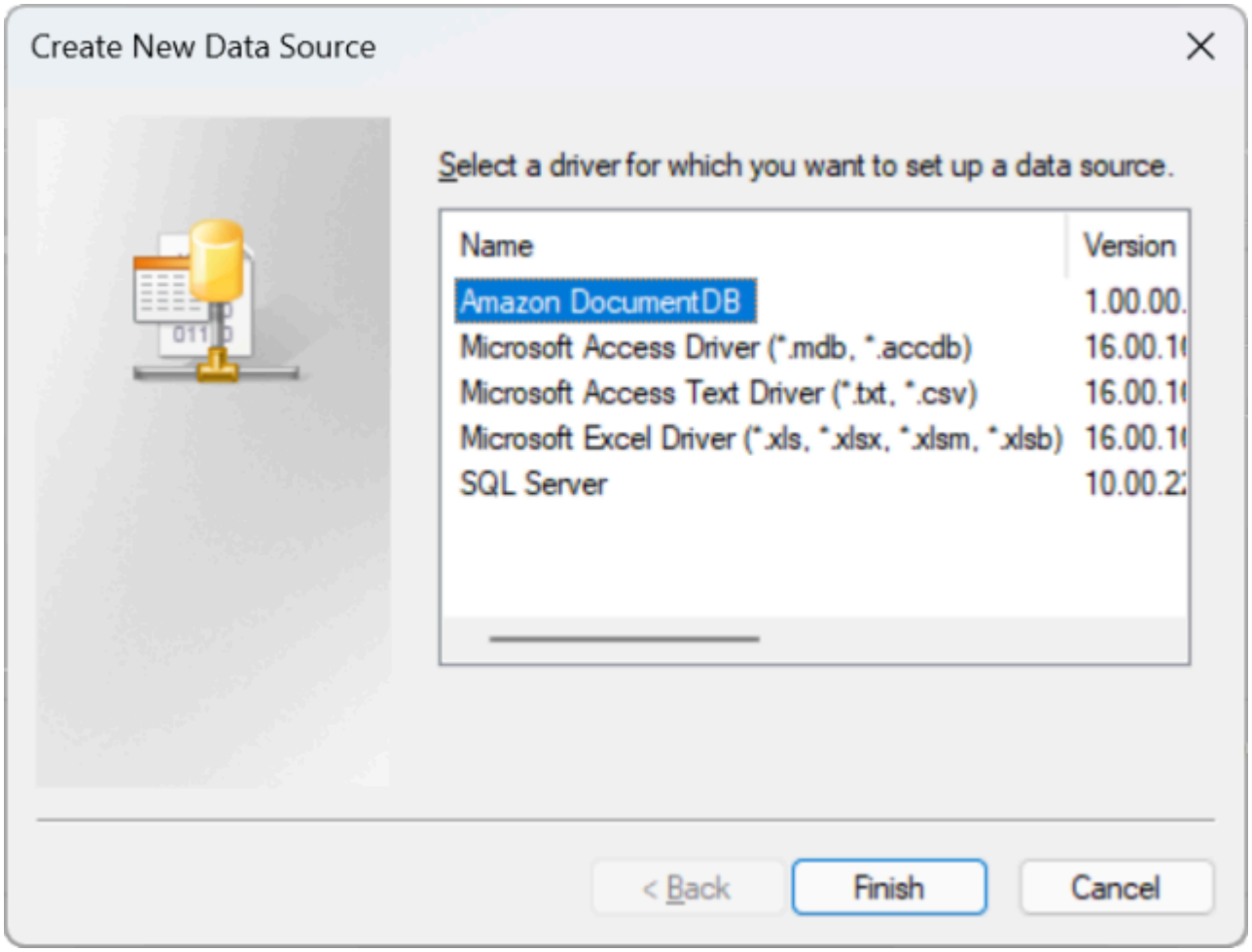
1. Abra el Panel de control en Windows y busque ODBC (o, en el menú, seleccione Herramientas de Windows > Fuentes de datos ODBC (32 bits) o Fuentes de datos ODBC (64 bits)):



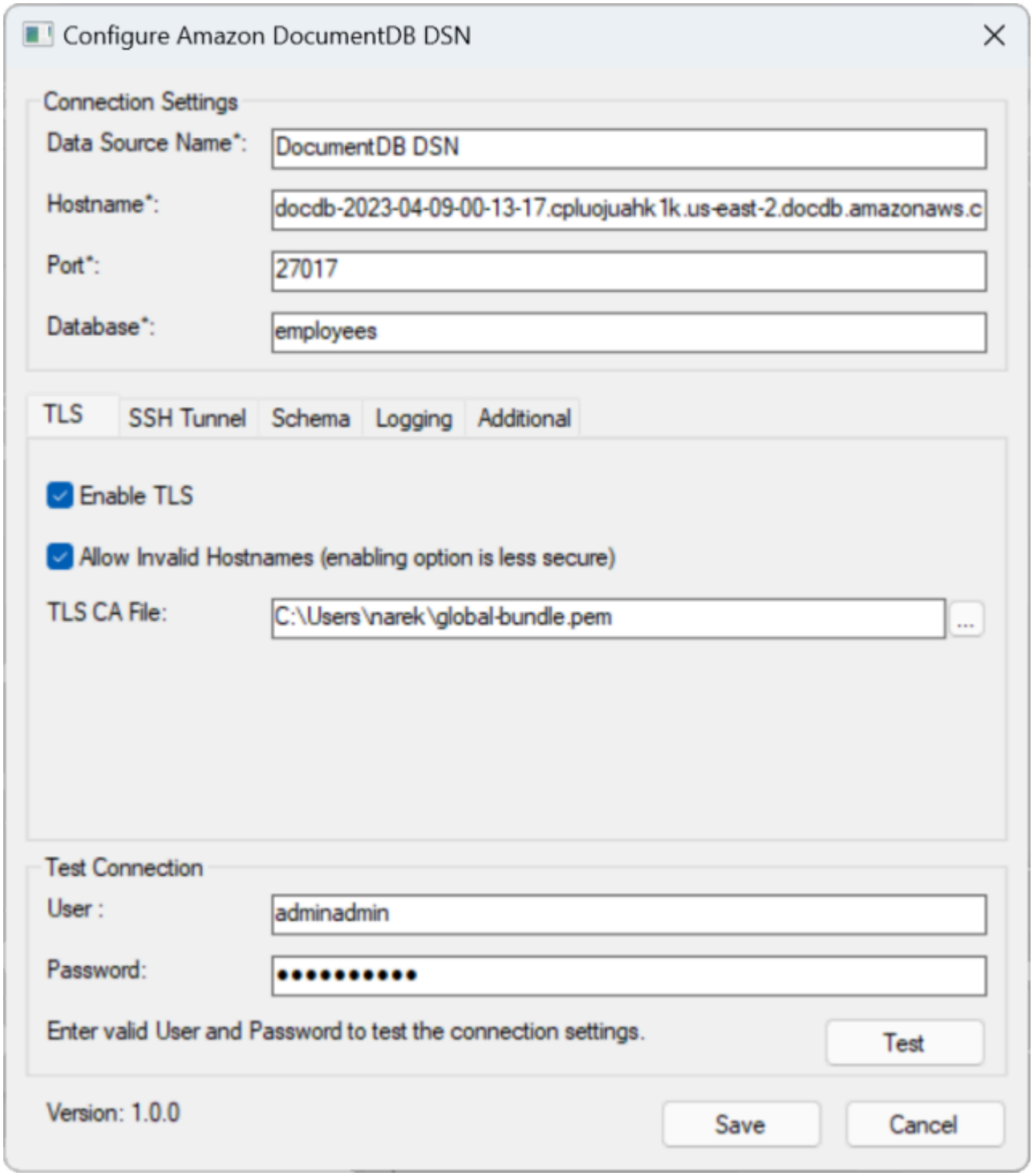
2. Seleccione el administrador de origen de datos del controlador ODBC adecuado: elija la versión de 32 bits si está instalada; de lo contrario, elija la versión de 64 bits.
3. Seleccione la pestaña DSN del sistema y, a continuación, haga clic en Agregar… para agregar un nuevo DSN:



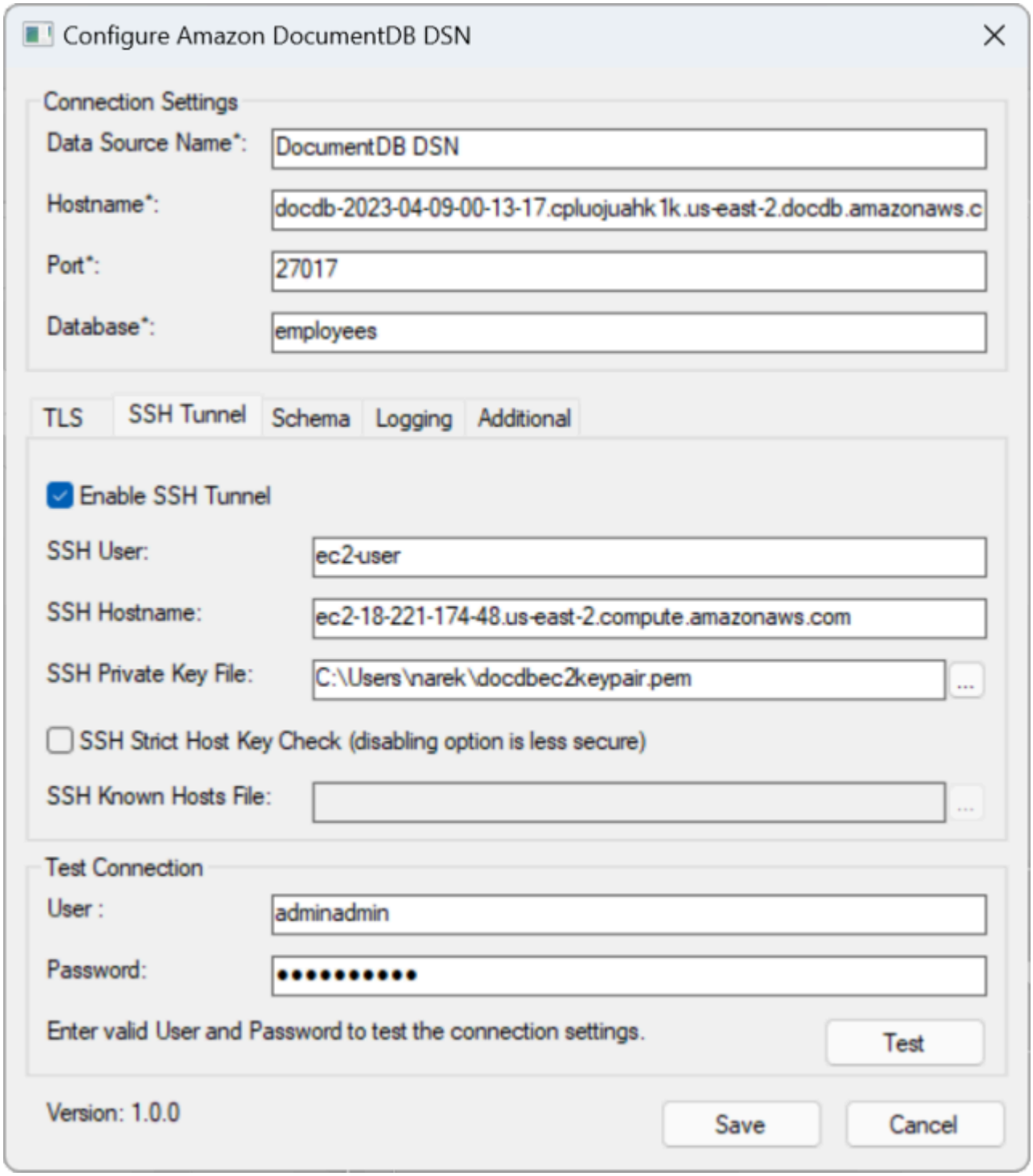
4. Elija Amazon DocumentDB en la lista de controladores de origen de datos:



5. En el cuadro de diálogo Configurar DSN de Amazon DocumentDB, complete los Ajustes de conexión, la pestaña TLS y los campos Probar conexión y, a continuación, haga clic en Guardar:



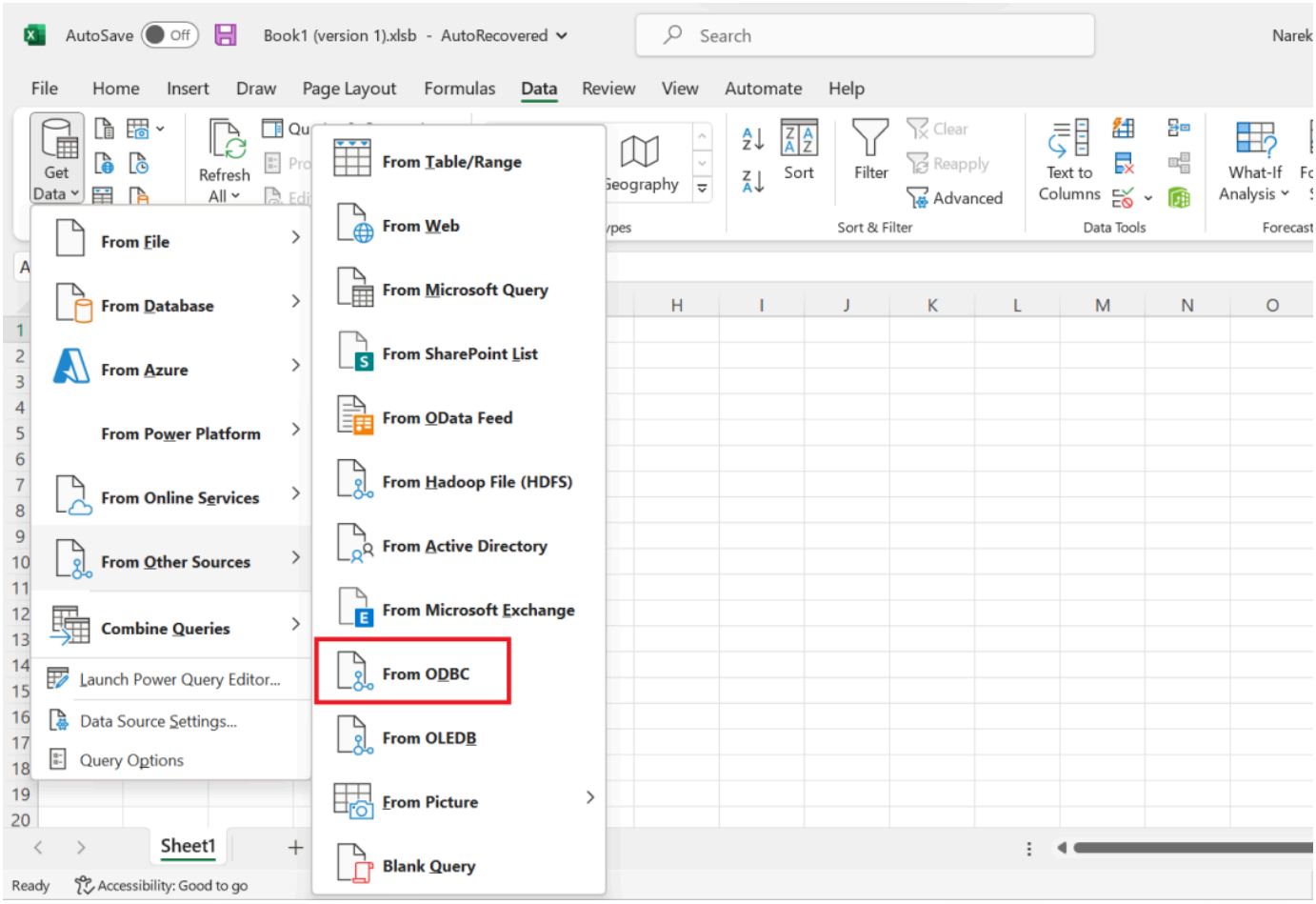
6. Asegúrese de completar el formulario de Windows correctamente, ya que los detalles de la conexión variarán según el método de tunelización SSH que haya elegido para la instancia EC2. Consulte los métodos de tunelización SSH aquí. Consulte Sintaxis y opciones de la cadena de conexión para obtener más información sobre cada propiedad.



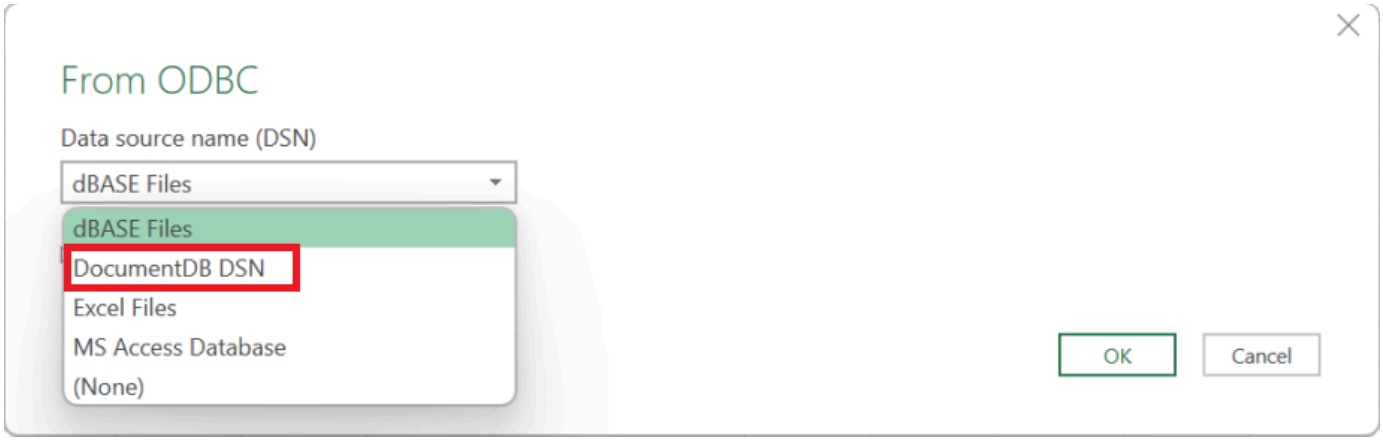
Para obtener más información sobre la configuración del controlador ODBC de Amazon DocumentDB en Windows, haga clic aquí.

Conexión a Amazon DocumentDB desde Microsoft Excel

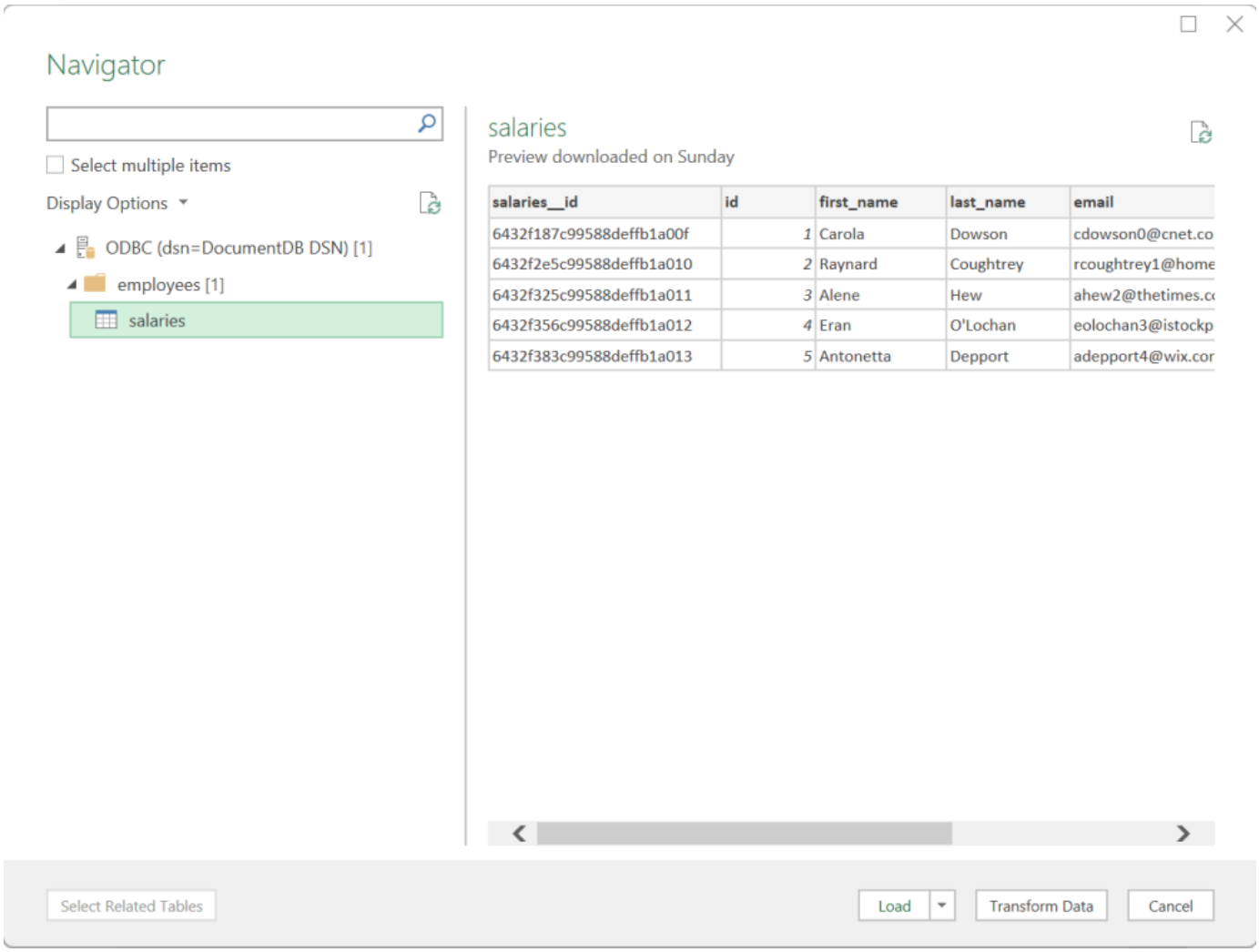
1. Asegúrese de que el controlador Amazon DocumentDB se haya instalado y configurado correctamente. Para obtener información adicional, consulte Configuración del controlador ODBC en Windows.
2. Abra Microsoft Excel.
3. Navegue hasta Datos > Obtener datos > De otras fuentes.
4. Elija Desde ODBC:



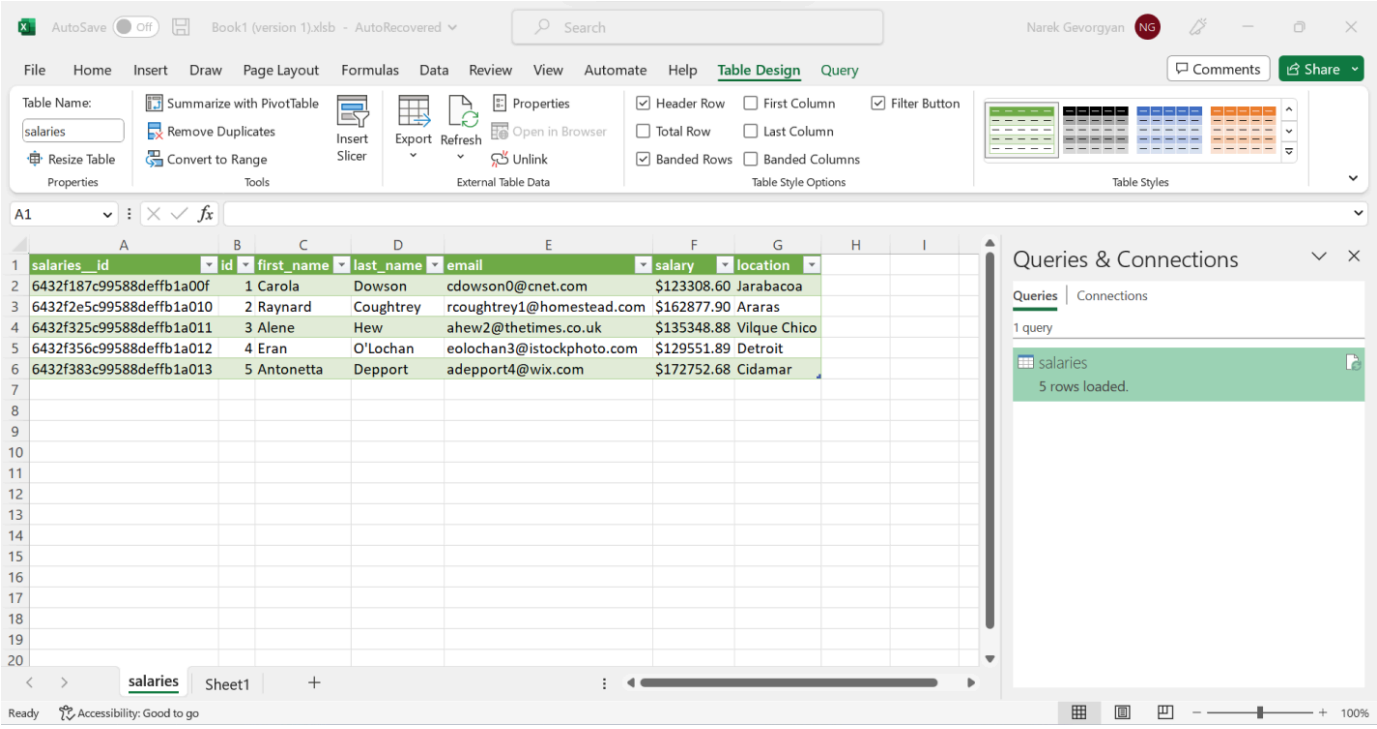
5. Seleccione el origen de datos en el menú desplegable Nombre del origen de datos (DSN) asociado a Amazon DocumentDB:



6. Elija la colección desde la que desea cargar datos en Excel:



7. Cargar datos en Excel:



Conexión a Amazon DocumentDB desde Power BI Desktop

Temas

- Requisitos previos
- Cómo añadir un conector personalizado de Microsoft Power BI Desktop
- Conexión mediante el conector personalizado de Amazon DocumentDB
- Configuración de la puerta de enlace Power BI de Microsoft

Requisitos previos

Antes de empezar, asegúrese de que el controlador ODBC de Amazon DocumentDB esté instalado correctamente.

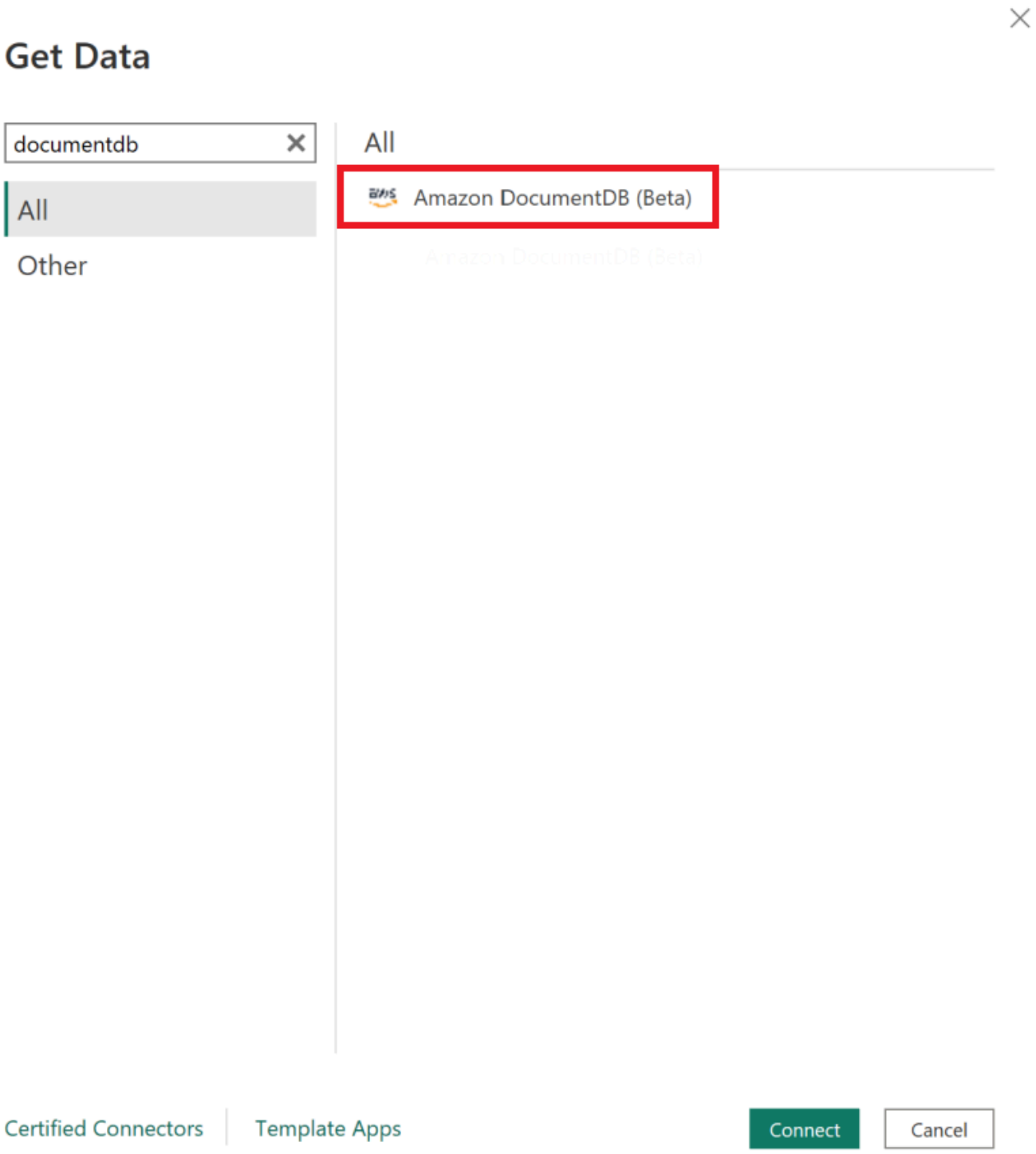
Cómo añadir un conector personalizado de Microsoft Power BI Desktop

Copie el archivo `AmazonDocumentDBConnector.mez` en la carpeta `<User>\Documents\Power BI Desktop\Custom Connectors\` (o `<User>\OneDrive\Documents\Power BI Desktop\Custom Connectors` si usa OneDrive). Esto permitirá a Power BI acceder al conector personalizado. Puede obtener el conector a Power BI Desktop aquí. Reinicie Power BI Desktop para asegurarse de que el conector esté cargado.

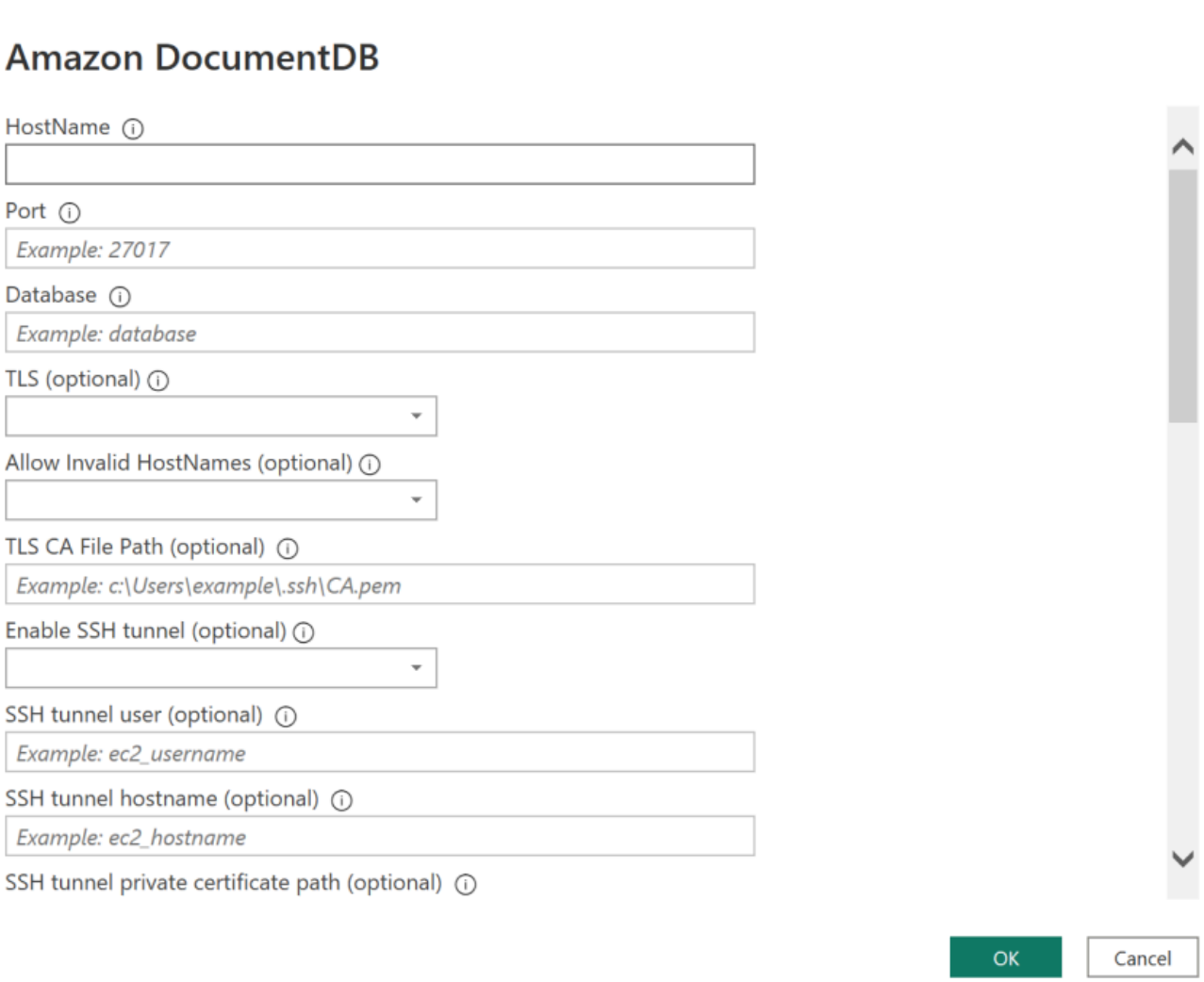
> **Note**
>
> El conector personalizado solo admite el nombre de usuario y la contraseña de Amazon DocumentDB para la autenticación.

Conexión mediante el conector personalizado de Amazon DocumentDB

1. Seleccione Amazon DocumentDB (Beta) en Obtener datos y haga clic en Conectar. Si recibe una advertencia por usar un servicio de terceros, haga clic en Continuar.



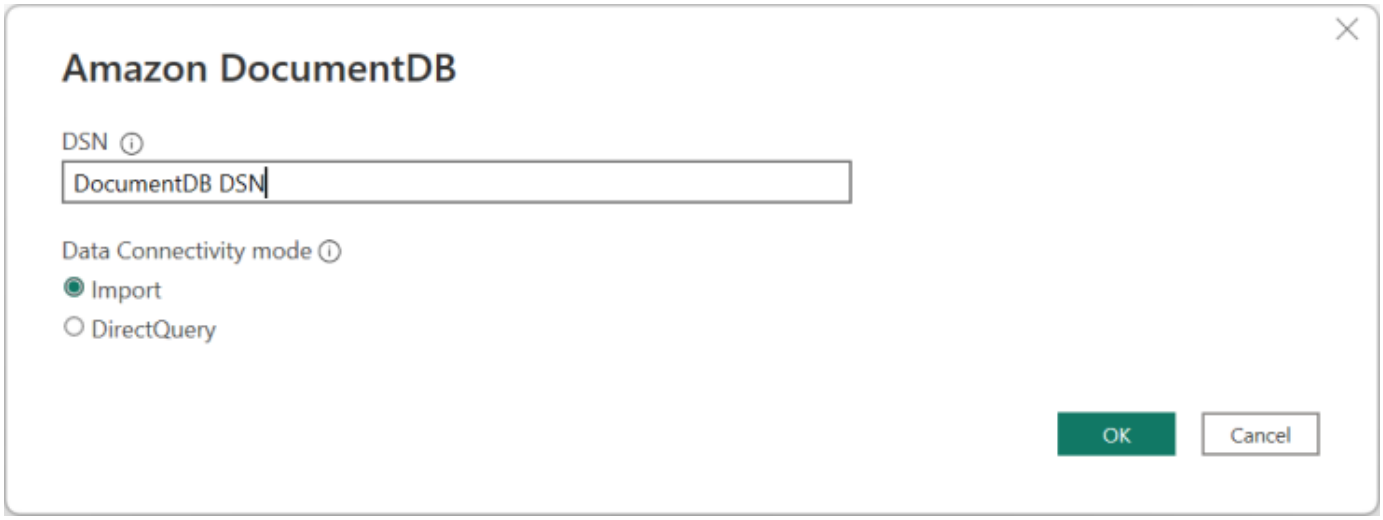
2. Introduzca toda la información necesaria para conectarse a su clúster de Amazon DocumentDB y, a continuación, haga clic en Aceptar:



> **Note**
>
> Según la configuración del nombre del origen de datos (DSN) del controlador ODBC, es posible que la pantalla de detalles de la conexión SSH no aparezca si ya ha proporcionado la información necesaria en la configuración del DSN.

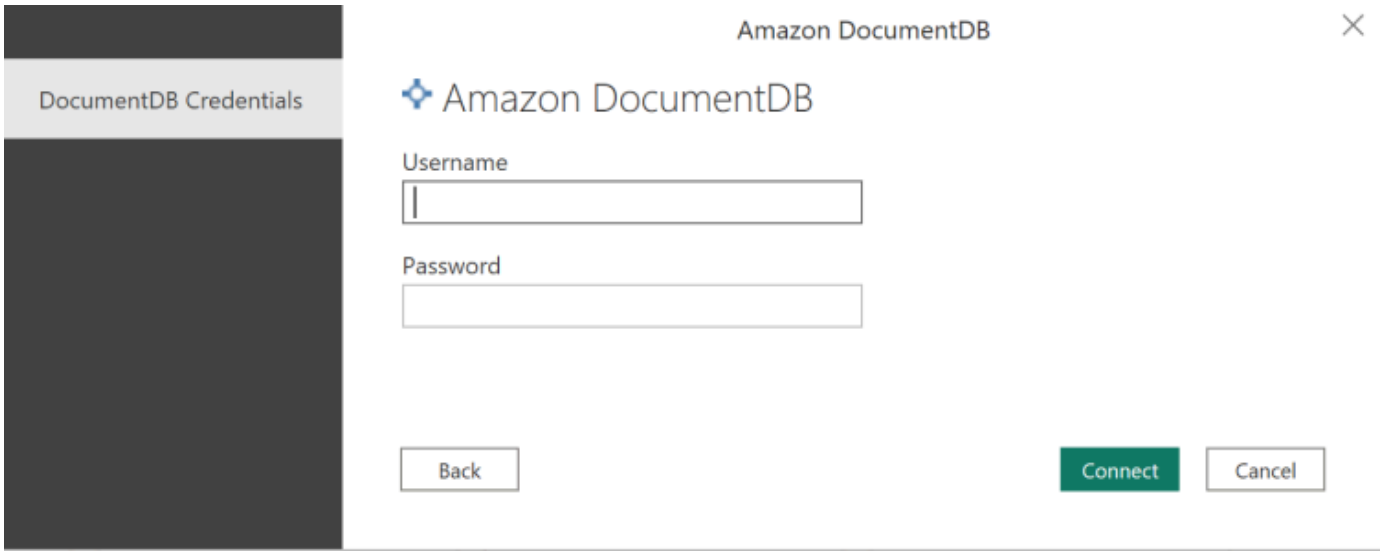
3. Seleccione el modo de conectividad de datos:

   - Importación: carga todos los datos y almacena la información en el disco. Los datos deben actualizarse y volver a cargarse para que se muestren las actualizaciones de datos.
   - Consulta directa: no carga datos, pero realiza consultas en tiempo real sobre los datos. Esto significa que no es necesario actualizar ni volver a cargar los datos para mostrar las actualizaciones de los datos.

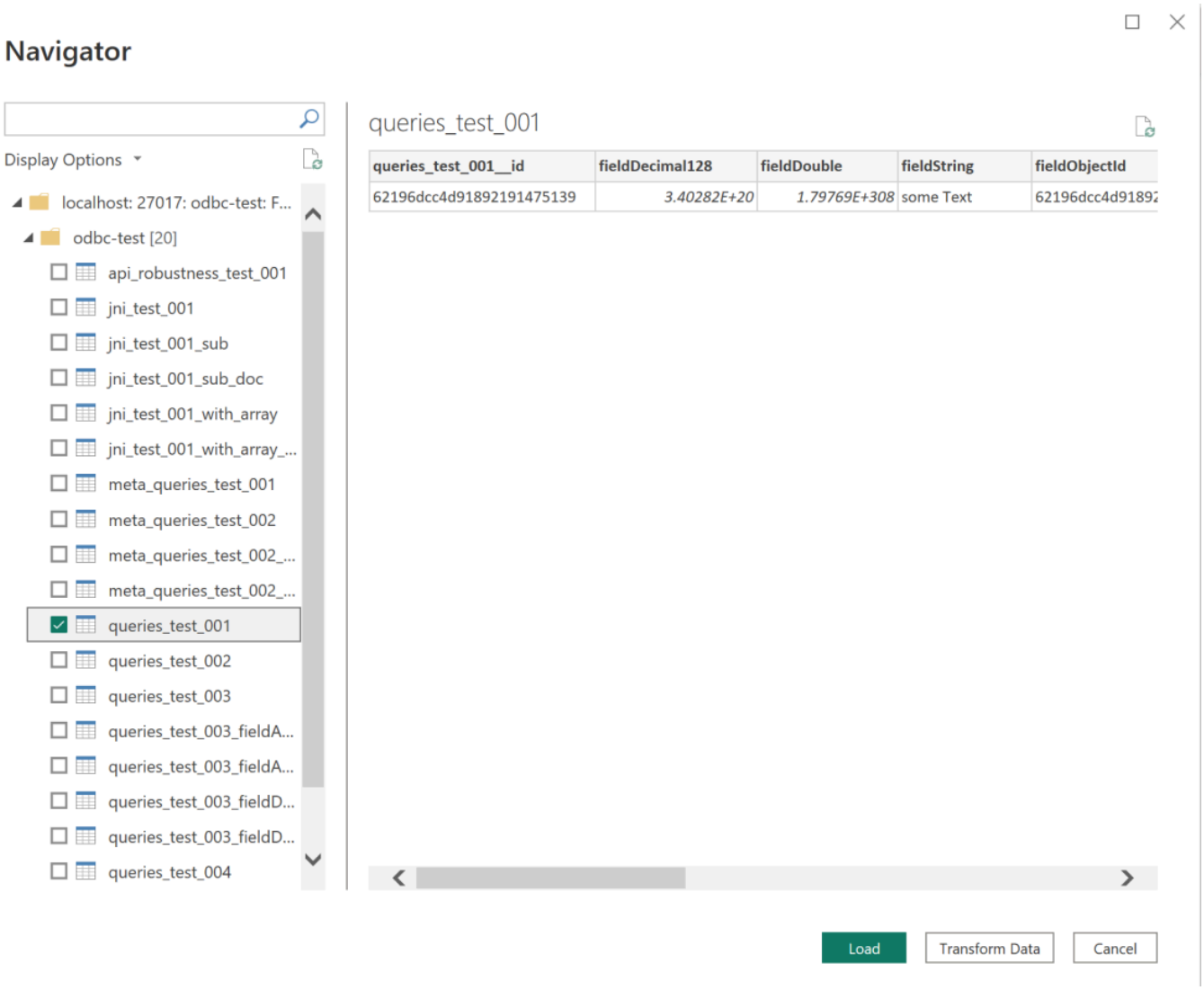


> **Note**
>
> Si utiliza un conjunto de datos muy grande, es posible que la importación de todos los datos tarde más tiempo.

4. Si es la primera vez que se conecta a este origen de datos, seleccione el tipo de autenticación e introduzca sus credenciales cuando así se le pida. A continuación, haga clic en Conectar:



5. En el cuadro de diálogo Navegador, seleccione las tablas de base de datos que desee y, a continuación, haga clic en Cargar para cargar los datos o en Transformar datos para continuar con la transformación de los datos.



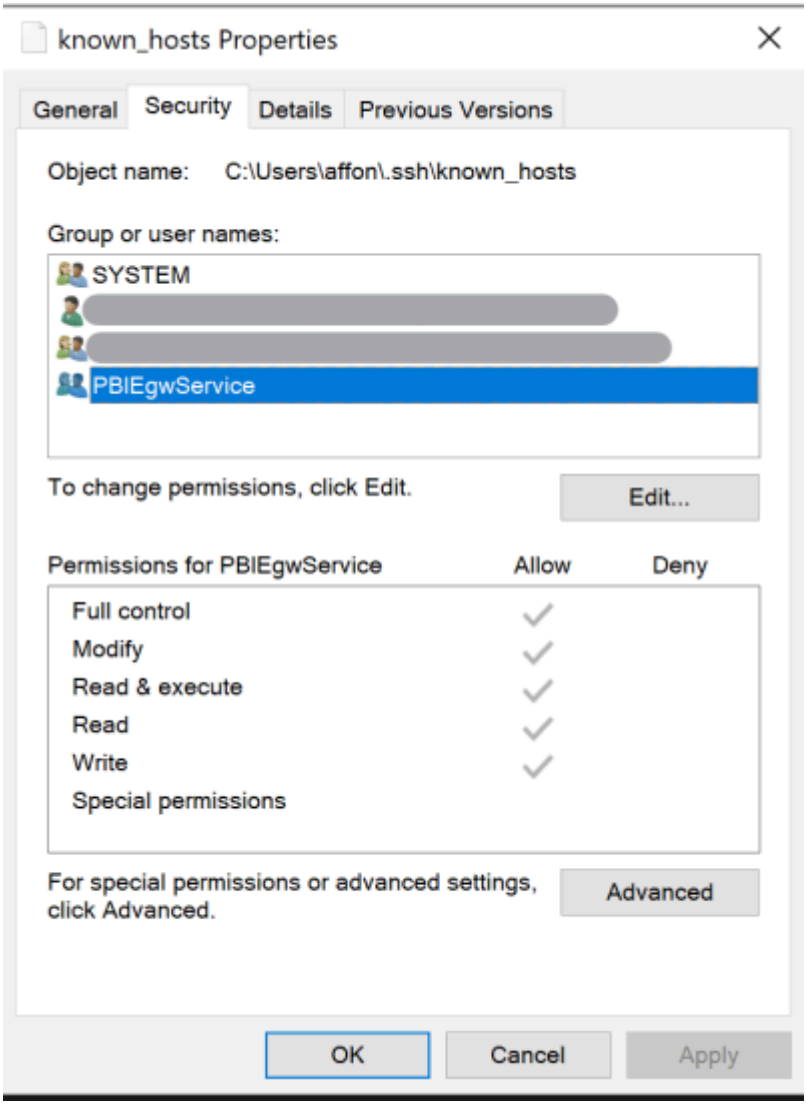
> **Note**
>
> La configuración del origen de datos se guarda una vez que se conecta. Para modificarlos, seleccione Transformar datos > Configuración del origen de datos.

Configuración de la puerta de enlace Power BI de Microsoft

Requisitos previos:

- Asegúrese de que el conector personalizado funcione con la puerta de enlace Power BI.
- Asegúrese de que el DSN de ODBC esté creado en el origen de datos de ODBC en la pestaña Sistema de la máquina en la que está instalada la puerta de enlace Power BI.

Si utiliza la característica de túnel SSH interno, el archivo `known_hosts` debe estar ubicado en un lugar donde la cuenta de servicio de Power BI tenga acceso a él.



> **Note**
>
> Esto también se aplica a cualquier archivo que necesite para poder establecer una conexión con su clúster de Amazon DocumentDB, como un archivo de certificado (archivo pem) de una autoridad de certificación (CA).

Generación automática de esquemas

El controlador ODBC utiliza el controlador JDBC de Amazon DocumentDB a través de JNI (interfaz nativa de Java), lo que hace que la característica de generación automática de esquemas funcione

de manera similar en el controlador JDBC. Para obtener más información sobre la generación automática de esquemas, consulte Generación automática de esquemas JDBC. Además, para obtener más información sobre la arquitectura del controlador ODBC, haga clic aquí.

Compatibilidad y limitaciones de SQL

El controlador ODBC de Amazon DocumentDB es un controlador de solo lectura que es compatible con un subconjunto de SQL-92 y algunas extensiones comunes. Consulte la documentación de Compatibilidad y limitaciones de ODBC para obtener más información.

Solución de problemas

Si tiene problemas al utilizar el controlador ODBC de Amazon DocumentDB, consulte la Guía de solución de problemas.

Programación con Amazon DocumentDB

El servicio admite la validación de esquemas JSON.

Temas

- Guía de programación de Amazon DocumentDB en Java
- Cómo utilizar la validación de esquemas JSON

Guía de programación de Amazon DocumentDB en Java

Esta guía completa proporciona una guía detallada para trabajar con Amazon DocumentDB mediante los controladores Java de MongoDB y abarca aspectos esenciales de las operaciones y la administración de bases de datos.

Temas

- Introducción
- Requisitos previos
- Modelos de datos para esta guía
- Conexión a Amazon DocumentDB con un controlador Java de MongoDB
- Realización de operaciones CRUD en Amazon DocumentDB con Java

- Administración de índices en Amazon DocumentDB con Java
- Programación basada en eventos con Amazon DocumentDB y Java

Introducción

La guía comienza con la conectividad y explica cómo establecer conexiones seguras a los clústeres de DocumentDB mediante el controlador Java de MongoDB. Detalla los componentes de la cadena de conexión, SSL/TLS la implementación y las diversas opciones de conexión, incluida la autenticación de IAM y la agrupación de conexiones, junto con estrategias sólidas de gestión de errores.

En la sección de operaciones CRUD (crear, leer, actualizar, eliminar) de la guía, se trata exhaustivamente la manipulación de documentos y muestra cómo crear, leer, actualizar y eliminar documentos mediante operaciones únicas o masivas. Se explica el uso de filtros, consultas y diversas opciones de operación, al tiempo que se hace hincapié en las mejores prácticas para la gestión de errores y la implementación de la lógica de reintento para mejorar la fiabilidad. La guía también cubre ampliamente la gestión de índices y detalla la creación y el mantenimiento de diferentes tipos de índices, incluidos los índices de un solo campo, compuestos, dispersos y de texto. Se explica cómo optimizar el rendimiento de las consultas mediante una selección adecuada de los índices y el uso de la función `explain()` para analizar los planes de ejecución de consultas.

La última sección se centra en la programación basada en eventos mediante los flujos de cambios de Amazon DocumentDB y demuestra cómo implementar la supervisión de cambios de datos en tiempo real en aplicaciones Java. Abarca la implementación de cursores de flujo de cambios, la gestión de los tokens de reanudación para un funcionamiento continuo y las operaciones basadas en el tiempo para el procesamiento de datos históricos. A lo largo de la guía, se proporcionan ejemplos de código prácticos y prácticas recomendadas, lo que la convierte en un recurso inestimable para crear aplicaciones sólidas en Java con Amazon DocumentDB.

Requisitos previos

Antes de empezar, asegúrese de que tiene lo siguiente:

- Una AWS cuenta con un clúster de DocumentDB configurado. Consulte esta entrada del blog de introducción para obtener información sobre la configuración del clúster de DocumentDB.
- El kit de desarrollo de Java (JDK) está instalado (utilizaremos Amazon Corretto 21 para esta guía).
- Maven para la administración de dependencias.

Modelos de datos para esta guía

Todo el código de ejemplo de esta guía presupone una conexión a una base de datos de prueba «ProgGuideData» que tiene la colección «Restaurantes». Todos los códigos de muestra de esta guía funcionan en un sistema de listas de restaurantes y, a continuación, se muestra un ejemplo del aspecto de un documento de este sistema:

```
{
    "_id": "ab6ad8f119b5bca3efa2c7ae",
    "restaurantId": "REST-CRT9BL",
    "name": "Thai Curry Palace",
    "description": "Amazing Restaurant, must visit",
    "cuisine": "Thai",
    "address": {
        "street": "914 Park Street",
        "city": "Bryan",
        "state": "AL",
        "zipCode": "96865",
        "location": {
            "type": "Point",
            "coordinates": [-25.4619, 8.389]
        }
    },
    "contact": {
        "phone": "(669) 915-9056 x6657"
    },
    "rating": {
        "average": 3.4,
        "totalReviews": 275
    },
    "priceRange": "$",
    "menu": [{
        "category": "Appetizers",
        "items": [{
            "name": "Buffalo Chicken Wings",
            "price": 13.42
        }]
    }],
    "features": [
        "Private Dining"
    ],
    "isActive": false“ michelin”: {“
        star”: 3,
```

```
        “ranking_years”: 4
    }
}
```

Todos los ejemplos de código que muestran las operaciones CRUD, la gestión de índices y la programación basada en eventos suponen que tiene un `dbClient` objeto de `MongoClient`, una `connectionDB` objeto de `MongoDatabase` y una `collection` objeto de `MongoCollection`.

> **Note**
>
> Todos los ejemplos de código de esta guía se han probado con el controlador Java de MongoDB, versión 5.3.0.

Conexión a Amazon DocumentDB con un controlador Java de MongoDB

En esta sección se proporciona una step-by-step guía para conectarse a Amazon DocumentDB mediante controladores Java. Esto le permitirá empezar a integrar DocumentDB en sus aplicaciones Java.

Temas

- Paso 1: Configuración del proyecto
- Paso 2: crear una cadena de conexión
- Paso 3: escribir el código de conexión
- Paso 4: gestionar excepciones de conexión
- Paso 5: ejecutar el código
- Prácticas recomendadas de conexión

Paso 1: Configuración del proyecto

1. Cree un proyecto java con Maven:

   ```
   mvn archetype:generate -DgroupId=com.docdb.guide -DartifactId=my-docdb-project -
   DarchetypeArtifactId=maven-archetype-quickstart -DinteractiveMode=false
   ```

2. Añada el controlador Java de MongoDB como una dependencia para el proyecto en su archivo «pom.xml»:

```
<dependency>
    <groupId>org.mongodb</groupId>
    <artifactId>mongodb-driver-sync</artifactId>
    <version>5.3.0</version>
</dependency>
```

Paso 2: crear una cadena de conexión

La cadena de conexión de Amazon DocumentDB es esencial para establecer una conexión entre la aplicación y el clúster de DocumentDB. Esta cadena encapsula información crucial, como el punto de conexión del clúster, el puerto, los detalles de autenticación y varias opciones de conexión. Para crear una cadena de conexión de DocumentDB, normalmente se empieza con el formato básico:

```
"mongodb://username:password@cluster-endpoint:port/?[connection options]"
```

Deberá sustituir los términos «nombre de usuario» y «contraseña» por sus credenciales reales. Puede encontrar el punto final y el número de puerto de su clúster Consola de administración de AWS tanto en el AWS CLI. Consulte Búsqueda de puntos de conexión de un clúster para encontrar el punto de conexión del clúster. El puerto 27017 es el puerto predeterminado de DocumentDB.

Ejemplos de cadenas de conexión

- Para establecer una conexión a DocumentDB mediante cifrado en tránsito y asegurarse de que las solicitudes de lectura vayan a las réplicas de lectura y escriban a la principal:

```
"mongodb://username:password@cluster-endpoint:27017/?tls=true&
   tlsCAFile=global-bundle.pem&
   readPreference=secondaryPreferred&
   retryWrites=false"
```

- Para establecer una conexión a DocumentDB mediante la autenticación de IAM:

```
"mongodb://cluster-endpoint:27017/?tls=true&
   tlsCAFile=global-bundle.pem&
   readPreference=secondaryPreferred&
   retryWrites=false&
   authSource=%24external&
   authMechanism=MONGODB-AWS"
```

Las diferentes opciones disponibles para la cadena de conexión son las siguientes:

- Certificado TLS
- Lectura a partir de réplicas de lectura
- Write concern y registro en diario
- RetryWrites
- Autenticación de IAM
- Grupo de conexiones
- Parámetros de tiempo de espera de conexión

Certificado TLS

`tls=true|false`: esta opción habilita o deshabilita la seguridad de la capa de transporte (TLS). De forma predeterminada, el cifrado en tránsito está habilitado en el clúster de Amazon DocumentDB y, por lo tanto, a menos que TLS esté deshabilitada en el nivel del clúster, el valor de esta opción debería ser `true`.

Cuando se utiliza TLS, el código debe proporcionar un certificado SSL cuando crea la conexión a un clúster de DocumentDB. Descargue el certificado necesario para realizar la conexión segura al clúster: `global-bundle.pem`. Hay dos formas de usar el archivo `global-bundle.pem`.

- Opción 1: extraer todos los certificados del archivo `global-bundle.pem` y usar la herramienta clave de Java para almacenarlos en un archivo `.jks` que luego se pueda usar en el código. Consulte la pestaña Java en Conexión con TLS habilitado para ver el script que muestra cómo hacerlo.
- Opción 2: añadir dinámicamente el archivo `global-bundle.pem` al código, crear un almacén de claves en memoria y usar `SSLContext` para proporcionar el certificado como parte de la conexión.

Lectura a partir de réplicas de lectura

`replicaSet=rs0&readPreference=secondaryPreferred`: si se especifican estas dos opciones, se redirigen todas las solicitudes de lectura a las réplicas de lectura y las solicitudes de escritura a la instancia principal. El uso de `replicaSet=rs0` en la cadena de conexión permite que el controlador MongoDB mantenga una vista actualizada automáticamente de la topología del clúster, lo que permite que las aplicaciones mantengan la visibilidad de las configuraciones de nodos actuales a medida que se añaden o eliminan instancias. Si no se proporcionan estas opciones ni

se especifica `readPreference=primary`, se envían todas las lecturas y escrituras a la instancia principal. Para obtener más opciones de `readPreference`, consulte Opciones de preferencia de lectura.

Write concern y registro en diario

La opción Write concern determina el nivel de reconocimiento solicitado a la base de datos para las operaciones de escritura. Los controladores MongoDB ofrecen una opción para ajustar los archivos de Write concern y de diario. Amazon DocumentDB no espera que establezca la opción de Write concern y diario, e ignora los valores enviados para `w` y `j` (`writeConcern` y `journal`). DocumentDB siempre escribe datos con `writeConcern`: `majority` y`journal`: `true` de modo que las escrituras se registren de forma duradera en la gran mayoría de los nodos antes de enviar una confirmación al cliente.

RetryWrites

`retryWrites=false`: DocumentDB no admite reintentos de escritura y, por lo tanto, este atributo siempre debe estar establecido en `false`.

Autenticación de IAM

`authSource=%24external`y **`authMechanism=MONGODB-AWS`**: estos dos parámetros se utilizan para autenticarse mediante AWS Identity and Access Management. En la actualidad, la autenticación de IAM está disponible solamente en la versión 5.0 del clúster basado en instancias. Para obtener más información, consulte Autenticación mediante la identidad de IAM.

Grupo de conexiones

Estas opciones están disponibles para la agrupación de conexiones:

- **`maxPoolSize`**: establece el número máximo de conexiones que se pueden crear en el grupo. Cuando todas las conexiones están en uso y llega una nueva solicitud, espera a que haya una conexión disponible. El valor predeterminado para los controladores Java de MongoDB es 100.
- **`minPoolSize`**: indica el número mínimo de conexiones que deben mantenerse en el grupo en todo momento. El valor predeterminado para los controladores Java de MongoDB es 0.
- **`maxIdleTimeMS`**: determina cuánto tiempo puede permanecer inactiva una conexión en el grupo antes de cerrarla y eliminarla. El valor predeterminado para los controladores Java de MongoDB es 100 milisegundos.
- **`waitQueueTimeoutMS`**: configura cuánto tiempo debe esperar un subproceso para que una conexión esté disponible cuando el grupo esté en su tamaño máximo. Si una conexión no

está disponible en este tiempo, se produce una excepción. El valor predeterminado para los controladores Java de MongoDB es 120 000 milisegundos (2 minutos).

Parámetros de tiempo de espera de conexión

El tiempo de espera es un mecanismo para limitar el tiempo que puede tardar una operación o un intento de conexión antes de que se considere fallido. Los siguientes parámetros de tiempo de espera están disponibles para evitar esperas indefinidas y administrar la asignación de recursos:

- **`connectTimeoutMS`**: configura cuánto tiempo esperará el controlador para establecer una conexión con el clúster. El valor predeterminado es de 10 000 milisegundos (10 segundos).
- **`socketTimeoutMS`**: especifica cuánto tiempo esperará el controlador para recibir una respuesta del servidor para una operación que no sea de escritura. El valor predeterminado es 0 (sin tiempo de espera o es infinito).
- **`serverSelectionTimeoutMS`**: especifica cuánto tiempo esperará el controlador para encontrar un servidor disponible en el clúster. El valor predeterminado de esta configuración es de 30 segundos y es suficiente para que se elija una nueva instancia principal durante la conmutación por error.

Paso 3: escribir el código de conexión

En el siguiente ejemplo de código se muestra cómo establecer una conexión de TLS a Amazon DocumentDB:

- Crea los objetos `KeyStore` y `SSLContext>` de Java.
- También crea el objeto `MongoClientSettings` pasándolo al objeto `ConnectionString`. Para establecer una conexión TLS, debe usar el objeto `MongoClientSettings` para vincular la `connectionstring` y el `sslcontext`.
- El uso de `MongoClients` obtiene un objeto `MongoClient`.

```
public static MongoClient makeDbConnection(String dbName, String DbUserName, String
 DbPassword,
    String DbClusterEndPoint, String keyStorePass) throws Exception {
    MongoClient connectedClient;
    String connectionOptions = "?
replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false";
```

```
    String connectionUrl = "mongodb://" + DbUserName + ":" + DbPassword + "@" +
 DbClusterEndPoint + ":27017/" +
        dbName + connectionOptions;

    try {
        KeyStore trustStore = KeyStore.getInstance(KeyStore.getDefaultType());
        try (FileInputStream fis = new FileInputStream("src/main/resources/certs/
truststore.jks")) {
            trustStore.load(fis, keyStorePass.toCharArray());
            TrustManagerFactory tmf =
 TrustManagerFactory.getInstance(TrustManagerFactory.getDefaultAlgorithm());
            tmf.init(trustStore);

            SSLContext sslContext = SSLContext.getInstance("TLSv1.2");
            sslContext.init(null, tmf.getTrustManagers(), new SecureRandom());
            ConnectionString connectionString = new ConnectionString(connectionUrl);
            MongoClientSettings settings = MongoClientSettings.builder()
                .applyConnectionString(connectionString)
                .applyToSslSettings(builder - > {
                    builder.enabled(true);
                    builder.context(sslContext);
                })
                .build();
            connectedClient = MongoClients.create(settings);
        }
        return connectedClient;
    } catch (MongoException e5) {
        throw new RuntimeException(e5);
    } catch (Exception e) {
        throw new RuntimeException(e);
    }
}
```

Paso 4: gestionar excepciones de conexión

Cuando se trabaja con DocumentDB en aplicaciones Java, el manejo de las excepciones de conexión es crucial para mantener operaciones de base de datos sólidas y fiables. Si se gestionan adecuadamente, estas excepciones no solo ayudan a diagnosticar los problemas rápidamente, sino que también garantizan que la aplicación pueda gestionar sin problemas las interrupciones temporales de la red o la falta de disponibilidad del servidor, lo que mejora la estabilidad y la experiencia del usuario. Algunas de las excepciones más importantes relacionadas con el establecimiento de la conexión son las siguientes:

- **`MongoException`**: es una excepción general y podría emitirse en varias situaciones no cubiertas por excepciones más específicas. Asegúrese de que esta excepción se gestione después de todas las demás excepciones específicas, ya que se trata de una excepción general de MongoDB.
- **`MongoTimeoutException`**: se emite cuando se agota el tiempo de espera de una operación. Por ejemplo, cuando consulta un punto de conexión de un clúster que no existe.
- **`MongoSocketException`**: se emite por problemas relacionados con la red. Por ejemplo, una desconexión repentina de la red durante una operación.
- **`MongoSecurityException`**: se emite cuando se produce un error en la autenticación. Por ejemplo, cuando se intenta conectar con credenciales incorrectas.
- **`MongoConfigurationException`**: se emite cuando hay un error en la configuración del cliente. Por ejemplo, si se utiliza una cadena de conexión no válida.

Paso 5: ejecutar el código

El siguiente ejemplo de código crea una conexión a Amazon DocumentDB e imprime todas las bases de datos:

```
public static void TestConnection() {
    try (MongoClient mongoClient = makeDbConnection(DATABASE_NAME, DB_USER_NAME,
 DB_PASSWORD, DB_CLUSTER_ENDPOINT, KEYSTORE_PASSWORD)) {
        List < String > databases = mongoClient.listDatabaseNames().into(new ArrayList
 < > ());
        System.out.println("Databases: " + databases);
    } catch (MongoException e) {
        System.err.println("MongoDB error: " + e.getMessage());
        throw new RuntimeException(e);
    }
}
```

Prácticas recomendadas de conexión

Las siguientes son prácticas recomendadas que se deben tener en cuenta cuando se conecta a Amazon DocumentDB con un controlador Java de MongoDB:

- Cierre siempre el `MongoClient` cuando ya no necesite que el cliente libere recursos.
- Gestione las excepciones de forma adecuada e implemente un registro de errores adecuado.
- Utilice variables de entorno o AWS Secrets Manager almacene información confidencial, como nombres de usuario y contraseñas.

Realización de operaciones CRUD en Amazon DocumentDB con Java

En esta sección se describe cómo realizar las operaciones CRUD (crear, leer, actualizar, eliminar) en Amazon DocumentDB con los controladores Java de MongoDB.

Temas

- Creación e inserción de documentos en una colección de DocumentDB
- Lectura y recuperación de datos de una colección de DocumentDB
- Actualización de documentos existentes en una colección de DocumentDB
- Eliminación de documentos de una colección de DocumentDB
- Gestión de errores con lógica de reintento

Creación e inserción de documentos en una colección de DocumentDB

La inserción de documentos en Amazon DocumentDB le permite añadir nuevos datos a sus colecciones. Existen varias formas de realizar las inserciones, en función de sus necesidades y del volumen de datos con el que esté trabajando. El método más básico para insertar un documento individual en la colección es `insertOne()`. Para insertar varios documentos a la vez, puede utilizar el método de `insertMany()`, que le permite añadir una serie de documentos en una sola operación. Otro método para insertar muchos documentos en una colección de DocumentDB es `bulkWrite()`. En esta guía, analizamos todos estos métodos para crear documentos en una colección de DocumentDB.

`insertOne()`

Empecemos por examinar cómo insertar un documento individual en una colección de Amazon DocumentDB. La inserción de un único documento se realiza mediante el método `insertOne()`. Este método toma un objeto BsonDocumentpara insertarlo y devuelve un `InsertOneResult`objeto que se puede utilizar para obtener el identificador de objeto del nuevo documento insertado. El siguiente código de ejemplo muestra la inserción de un documento de restaurante en la colección:

```
Document article = new Document()
    .append("restaurantId", "REST-21G145")
    .append("name", "Future-proofed Intelligent Bronze Hat")
    .append("cuisine", "International")
    .append("rating", new Document()
        .append("average", 1.8)
```

```
        .append("totalReviews", 267))
    .append("features", Arrays.asList("Outdoor Seating", "Live Music"));

try {
    InsertOneResult result = collection.insertOne(article);
    System.out.println("Inserted document with the following id: " +
 result.getInsertedId());
} catch (MongoWriteException e) {
    // Handle duplicate key or other write errors
    System.err.println("Failed to insert document: " + e.getMessage());
    throw e;
} catch (MongoException e) {
    // Handle other MongoDB errors
    System.err.println("MongoDB error: " + e.getMessage());
    throw e;
}
```

Cuando use `insertOne()`, asegúrese de incluir una gestión de errores adecuada. Por ejemplo, en el código anterior, «`restaurantId`» tiene un índice único y, por lo tanto, cuando vuelva a ejecutar este código, se generará la siguiente `MongoWriteException`:

```
Failed to insert document: Write operation error on server
 docdbCluster.docdb.amazonaws.com:27017.
Write error: WriteError{code=11000, message='E11000 duplicate key error collection:
 Restaurants index: restaurantId_1', details={}}.
```

InsertMany()

Los métodos principales utilizados para insertar muchos documentos en una colección son insertMany() y `bulkWrite()`.

El método `insertMany()` es la forma más sencilla de insertar varios documentos en una sola operación. Acepta una lista de documentos y los inserta en la colección. Este método es ideal cuando se inserta un lote de documentos nuevos que son independientes entre sí y no requieren ningún procesamiento especial ni operaciones mixtas. El siguiente código muestra la lectura de documentos JSON de un archivo y su inserción en la colección. La `insertMany()` función devuelve un `InsertManyResult`objeto que se puede utilizar para obtener todos IDs los documentos insertados.

```
// Read JSON file content
String content = new String(Files.readAllBytes(Paths.get(jsonFileName)));
```

```
JSONArray jsonArray = new JSONArray(content);

// Convert JSON articles to Documents
List < Document > restaurants = new ArrayList < > ();
for (int i = 0; i < jsonArray.length(); i++) {
    JSONObject jsonObject = jsonArray.getJSONObject(i);
    Document doc = Document.parse(jsonObject.toString());
    restaurants.add(doc);
}
//insert documents in collection
InsertManyResult result = collection.insertMany(restaurants);

System.out.println("Count of inserted documents: " + result.getInsertedIds().size());
```

bulkWrite()

El método `bulkWrite()` permite realizar múltiples operaciones de escritura (insertar, actualizar, eliminar) en un solo lote. Puede usar `bulkWrite()` cuando necesite realizar diferentes tipos de operaciones en un solo lote, como insertar algunos documentos y actualizar otros. `bulkWrite()` admite dos tipos de escritura por lotes, ordenada y desordenada:

- Operaciones ordenadas (predeterminado): Amazon DocumentDB procesa las operaciones de escritura de forma secuencial y se detiene ante el primer error que detecta. Esto resulta útil cuando el orden de las operaciones es importante, por ejemplo, cuando las operaciones posteriores dependen de las anteriores. Sin embargo, las operaciones ordenadas suelen ser más lentas que las desordenadas. En el caso de las operaciones ordenadas, debe abordar el caso de que el lote se detenga ante el primer error, lo que podría dejar algunas operaciones sin procesar.
- Operaciones desordenadas: permite a Amazon DocumentDB procesar las inserciones como una sola ejecución en la base de datos. Si se produce un error en un documento, la operación continúa con el resto de los documentos. Esto resulta especialmente útil cuando se insertan grandes cantidades de datos y se pueden tolerar algunos errores, como durante la migración de datos o las importaciones masivas, donde algunos documentos pueden fallar debido a la duplicación de claves. En el caso de operaciones desordenadas, debe abordar las situaciones de éxito parcial, en los que algunas operaciones se realizan correctamente y otras no.

Al trabajar con el método `bulkWrite()`, se requieren algunas clases esenciales. En primer lugar, la clase `WriteModel` sirve como clase base para todas las operaciones de escritura y tiene implementaciones específicas como `InsertOneModel`, `UpdateOneModel`, `UpdateManyModel`, `DeleteOneModel` y `DeleteManyModel`, que manejan diferentes tipos de operaciones.

La BulkWriteOptionsclase es necesaria para configurar el comportamiento de las operaciones masivas, como configurar la ordered/unordered ejecución o omitir la validación de los documentos. La clase BulkWriteResult proporciona información detallada sobre los resultados de la ejecución, incluidos los recuentos de documentos insertados, actualizados y eliminados.

Para la gestión de errores, la clase MongoBulkWriteException es fundamental, ya que contiene información sobre los posibles errores que se produzcan durante la operación masiva, mientras que la clase BulkWriteError proporciona detalles específicos sobre los errores de las operaciones individuales. El siguiente código muestra un ejemplo de inserción de una lista de documentos, así como de actualización y eliminación de un solo documento, todo ello mediante la ejecución de una llamada a un único método `bulkWrite()`. El código también muestra cómo trabajar con BulkWriteOptions y BulkWriteResult, así como la correcta gestión de errores de la operación de `bulkWrite()`.

```
List < WriteModel < Document >> bulkOperations = new ArrayList < > ();
// get list of 10 documents representing 10 restaurants
List < Document > restaurantsToInsert = getSampleData();

for (Document doc: restaurantsToInsert) {
    bulkOperations.add(new InsertOneModel < > (doc));
}
// Update operation
bulkOperations.add(new UpdateOneModel < > (
    new Document("restaurantId", "REST-Y2E9H5"),
    new Document("", new Document("stats.likes", 20))
    .append("", new Document("rating.average", 4.5))));
// Delete operation
bulkOperations.add(new DeleteOneModel < > (new Document("restaurantId", "REST-
D2L431")));

// Perform bulkWrite operation
try {
    BulkWriteOptions options = new BulkWriteOptions()
        .ordered(false); // Allow unordered inserts

    BulkWriteResult result = collection.bulkWrite(bulkOperations, options);

    System.out.println("Inserted: " + result.getInsertedCount());
    System.out.println("Updated: " + result.getModifiedCount());
    System.out.println("Deleted: " + result.getDeletedCount());
} catch (MongoBulkWriteException e) {
    System.err.println("Bulk write error occurred: " + e.getMessage());
```

```
    // Log individual write errors
    for (BulkWriteError error: e.getWriteErrors()) {
        System.err.printf("Error at index %d: %s (Code: %d)%n", error.getIndex(),
 error.getMessage(),
            error.getCode());

        // Log the problematic document
        Document errorDoc = new Document(error.getDetails());
        if (errorDoc != null) {
            System.err.println("Problematic document: " + errorDoc);
        }
    }
} catch (Exception e) {
    System.err.println("Error during bulkWrite: " + e.getMessage());
}
```

Escrituras reintentables

A diferencia de MongoDB, Amazon DocumentDB no admite el reintento de las escrituras. En consecuencia, debe implementar una lógica de reintento personalizada en sus aplicaciones, especialmente para solucionar problemas de red o la falta temporal de disponibilidad del servicio. Por lo general, una estrategia de reintentos bien implementada implica aumentar la demora entre los reintentos y limitar el número total de reintentos. Consulte Gestión de errores con lógica de reintento a continuación para conocer un ejemplo de código sobre cómo crear una lógica de reintentos con gestión de errores.

Lectura y recuperación de datos de una colección de DocumentDB

La consulta de documentos en Amazon DocumentDB gira en torno a varios componentes clave que permiten recuperar y manipular datos con precisión. El `find()`método es la consulta fundamental APIs en los controladores Java de MongoDB. Permite la recuperación de datos complejos con numerosas opciones para filtrar, ordenar y proyectar resultados. Además del método `find()`, `Filters` y `FindIterable` son otros dos componentes fundamentales que proporcionan los componentes básicos para las operaciones de consulta en los controladores Java de MongoDB.

La clase `Filters` es una clase de utilidad del controlador Java de MongoDB que proporciona una API fluida para generar un constructo de filtros de consultas. Esta clase ofrece métodos de fábrica estáticos que crean instancias de objetos `Bson` que representan diversas condiciones de consulta. Los métodos más comúnmente utilizados son `eq()` para las comparaciones de igualdad, `gt()`, `lt()`, `gte()` y `lte()` para las comparaciones numéricas, `and()` y `or()` para las combinaciones de condiciones múltiples, `in()` y `nin()` para las pruebas de suscripción a matrices y `regex()`

para la coincidencia de patrones. La clase está diseñada para ser segura en relación con los tipos y proporciona una mejor comprobación en tiempo de compilación en comparación con las consultas basadas en documentos sin procesar, lo que la convierte en el enfoque preferido para crear consultas de DocumentDB en aplicaciones Java. La gestión de errores es sólida, con claras excepciones en el caso de constructos de filtros no válidas.

`FindIterable` es una interfaz especializada diseñada para gestionar el resultado del método `find()`. Proporciona un amplio conjunto de métodos para refinar y controlar la ejecución de consultas, y ofrece una API fluida para el encadenamiento de métodos. La interfaz incluye métodos esenciales de modificación de consultas, como `limit()` para restringir el número de documentos devueltos, `skip()` para paginar, `sort()` para ordenar los resultados, `projection()` para seleccionar campos específicos y `hint()` para seleccionar índices. Las operaciones de agrupar en lotes, omitir y limitar en `FindIterable` son herramientas esenciales de paginación y administración de datos que ayudan a controlar la forma en que se recuperan y procesan los documentos de la base de datos.

Agrupar en lotes (`batchSize`) controla el número de documentos que DocumentDB devuelve al cliente en una única red de ida y vuelta. Cuando establece un tamaño de lote, DocumentDB no devuelve todos los documentos coincidentes a la vez, sino que los devuelve en grupos del tamaño de lote especificado.

Omitir le permite desplazar el punto de partida de los resultados y, básicamente, le indica a DocumentDB que omita un número específico de documentos antes de empezar a devolver las coincidencias. Por ejemplo, `skip(20)` omitirá los primeros 20 documentos coincidentes. Esto se suele utilizar en situaciones de paginación en los que se desean recuperar páginas de resultados posteriores.

Limitar restringe el número total de documentos que se pueden devolver a partir de una consulta. Si especifica `limit(n)`, DocumentDB dejará de devolver documentos después de haber devuelto «n» documentos, incluso si hay más coincidencias en la base de datos.

`FindIterable` admite patrones de iterador y cursor cuando recupera documentos de Amazon DocumentDB. La ventaja de usar `FindIterable` como iterador es que permite la carga diferida de los documentos y solo los recupera cuando la aplicación los solicita. Otra ventaja de usar el iterador es que no es responsable de mantener la conexión con el clúster y, por lo tanto, no es necesario cerrar la conexión de forma explícita.

`FindIterable` también proporciona soporte para `MongoCursor`, que permite utilizar patrones de cursor cuando trabaja con consultas de Amazon DocumentDB. El `MongoCursor` es una

implementación específica del controlador Java de MongoDB que proporciona control sobre las operaciones de la base de datos y la administración de recursos. Implementa la `AutoCloseable` interfaz, lo que permite una gestión explícita de los recursos mediante try-with-resources bloques, lo cual es crucial para cerrar correctamente las conexiones de las bases de datos y liberar los recursos del servidor. De forma predeterminada, el tiempo de espera del cursor es de 10 minutos y DocumentDB no le da la opción de cambiar este comportamiento de tiempo de espera. Cuando trabaje con datos agrupados, asegúrese de recuperar el siguiente lote de datos antes de que se agote el tiempo de espera del cursor. Una consideración clave a la hora de usar el `MongoCursor` es que requiere un cierre explícito para evitar la pérdida de recursos.

En esta sección, se presentan varios ejemplos de `find()`, `Filters` y `FindIterable`.

En el siguiente ejemplo de código se muestra cómo usar `find()` para recuperar un solo documento con su campo «restaurantId»:

```
Document filter = new Document("restaurantId", "REST-21G145");
Document result = collection.find(filter).first();
```

Si bien el uso de `Filters` permite comprobar mejor los errores en el momento de la compilación, el controlador java también permite especificar un filtro de `Bson` directamente en el método `find()`. El siguiente código de ejemplo pasa el documento `Bson` a `find()`:

```
result = collection.find(new Document("$and", Arrays.asList(
    new Document("rating.totalReviews", new Document("$gt", 1000)),
    new Document("priceRange", "$$"))))
```

El siguiente código de ejemplo muestra varios ejemplos del uso de la clase `Filters` con `find()`:

```
FindIterable < Document > results;

// Exact match
results = collection.find(Filters.eq("name", "Thai Curry Palace"));

// Not equal
results = collection.find(Filters.ne("cuisine", "Thai"));

// find an element in an array
results = collection.find(Filters.in("features", Arrays.asList("Private Dining")));

// Greater than
```

```
results = collection.find(Filters.gt("rating.average", 3.5));

// Between (inclusive)
results = collection.find(Filters.and(
    Filters.gte("rating.totalReviews", 100),
    Filters.lte("rating.totalReviews", 200)));
// AND
results = collection.find(Filters.and(
    Filters.eq("cuisine", "Thai"),
    Filters.gt("rating.average", 4.5)));

// OR
results = collection.find(Filters.or(
    Filters.eq("cuisine", "Thai"),
    Filters.eq("cuisine", "American")));


// All document where the Field exists
results = collection.find(Filters.exists("michelin"));

// Regex
results = collection.find(Filters.regex("name", Pattern.compile("Curry",
 Pattern.CASE_INSENSITIVE)));

// Find all document where the array contain the list of value regardless of its order
results = collection.find(Filters.all("features", Arrays.asList("Private Dining",
 "Parking")));

// Array size
results = collection.find(Filters.size("features", 4));
```

En el siguiente ejemplo se muestra cómo encadenar las operaciones de `sort()`, `skip()`, `limit()` y `batchSize()` en un objeto de `FindIterable`. El orden en que se proporcionen estas operaciones influirá en el rendimiento de la consulta. Como práctica recomendada, el orden de estas operaciones debe ser `sort()`, `projection()`, `skip()`, `limit()` y `batchSize()`.

```
FindIterable < Document > results = collection.find(Filters.gt("rating.totalReviews",
 1000))
    // Sorting
    .sort(Sorts.orderBy(
        Sorts.descending("address.city"),
        Sorts.ascending("cuisine")))
    // Field selection
```

```
    .projection(Projections.fields(
        Projections.include("name", "cuisine", "priceRange"),
        Projections.excludeId()))

    // Pagination
    .skip(20)
    .limit(10)
    .batchSize(2);
```

El siguiente ejemplo de código muestra cómo crear un iterador en `FindIterable`. Usa el constructo `forEach` de Java para recorrer el conjunto de resultados.

```
collection.find(Filters.eq("cuisine", "American")).forEach(doc ->
 System.out.println(doc.toJson()));
```

En el último ejemplo de código de `find()`, se muestra cómo usar el `cursor()` para la recuperación de documentos. Crea el cursor en el bloque de prueba, lo que garantiza que el cursor se cierre cuando el código salga del bloque de prueba.

```
try (MongoCursor < Document > cursor = collection.find(Filters.eq("cuisine",
 "American"))
    .batchSize(25)
    .cursor()) {
    while (cursor.hasNext()) {
        Document doc = cursor.next();
        System.out.println(doc.toJson());
    }
} // Cursor automatically closed
```

Actualización de documentos existentes en una colección de DocumentDB

Amazon DocumentDB proporciona mecanismos flexibles y potentes para modificar los documentos existentes e insertar otros nuevos cuando no existen. El controlador Java de MongoDB ofrece varios métodos de actualización: `updateOne()` para actualizaciones de un solo documento, `updateMany()` para actualizaciones de varios documentos y `replaceOne()` para la sustitución completa de documentos. Además de estos tres métodos, `Updates`, `UpdateOptions` y `UpdateResult` son otros componentes fundamentales que proporcionan los componentes básicos para las operaciones de actualización en los controladores Java de MongoDB.

La clase `Updates` del controlador Java de MongoDB es una clase de utilidad que proporciona métodos de fábrica estáticos para crear operadores de actualización. Sirve como el compilador

principal para crear operaciones de actualización de forma legible y segura. Métodos básicos como `set()`, `unset()` y `inc()` permiten la modificación directa de los documentos. El poder de esta clase se hace evidente cuando se combinan varias operaciones mediante el método `Updates.combine()`, que permite ejecutar varias operaciones de actualización de forma atómica, lo que garantiza la coherencia de datos.

`UpdateOptions` es una potente clase de configuración del controlador Java de MongoDB que proporciona capacidades de personalización esenciales para las operaciones de actualización de documentos. Dos aspectos importantes de esta clase son la compatibilidad con actualizaciones y filtros de matriz para las operaciones de actualización. La característica de actualización, habilitada mediante `upsert(true)`, permite crear nuevos documentos cuando no se encuentra ningún documento coincidente durante una operación de actualización. Mediante `arrayFilters()`, la operación de actualización puede actualizar con precisión los elementos de la matriz que cumplan criterios específicos.

`UpdateResult` en el controlador Java de MongoDB proporciona el mecanismo de retroalimentación que detalla el resultado de una operación de actualización. Esta clase agrupa tres métricas clave: el número de documentos que cumplen los criterios de actualización (`matchedCount`), el número de documentos realmente modificados (`modifiedCount`) y la información sobre cualquier documento alterado (`upsertedId`). Comprender estas métricas es esencial para gestionar correctamente los errores, verificar las operaciones de actualización y mantener la coherencia de datos en las aplicaciones.

Actualización y sustitución de un solo documento

En DocumentDB, la actualización de un solo documento se puede realizar mediante el método updateOne(). Este método utiliza un parámetro de filtro, normalmente proporcionado por la clase `Filters`, para identificar el documento que se va a actualizar, un parámetro de `Updat` que determina qué campos se van a actualizar y un parámetro de `UpdateOptions` opcional para establecer diferentes opciones de actualización. El uso del método `updateOne()` solo actualizará el primer documento que coincida con los criterios de selección. El siguiente código de ejemplo actualiza un solo campo de un documento:

```
collection.updateOne(Filters.eq("restaurantId", "REST-Y2E9H5"),
    Updates.set("name", "Amazing Japanese sushi"));
```

Para actualizar varios campos de un documento, use `updateOne()` con `Update.combine()` como se muestra en el siguiente ejemplo. En este ejemplo también se muestra cómo agregar un elemento a una matriz del documento.

```
List<Bson> updates = new ArrayList<>();
// Basic field updates
updates.add(Updates.set("name", "Shanghai Best"));
// Array operations
updates.add(Updates.addEachToSet("features", Arrays.asList("Live Music")));
// Counter updates
updates.add(Updates.inc("rating.totalReviews", 10));
// Combine all updates
Bson combinedUpdates = Updates.combine(updates);
// Execute automic update with one call
collection.updateOne(Filters.eq("restaurantId","REST-1J83NH"), combinedUpdates);
```

En el siguiente ejemplo de código se muestra cómo actualizar un documento de la base de datos. Si el documento especificado no existe, la operación lo insertará automáticamente como documento nuevo. Este código también muestra cómo utilizar las métricas disponibles a través del objeto de `UpdateResult`.

```
Bson filter = Filters.eq("restaurantId", "REST-0Y9GL0");
Bson update = Updates.set("cuisine", "Indian");
// Upsert operation
UpdateOptions options = new UpdateOptions().upsert(true);
UpdateResult result = collection.updateOne(filter, update, options);

if (result.getUpsertedId() != null) {
    System.out.println("Inserted document with _id: " + result.getUpsertedId());
} else {
     System.out.println("Updated " + result.getModifiedCount() + " document(s)");
}
```

El siguiente ejemplo de código muestra cómo reemplazar completamente un documento existente por uno nuevo mediante el método `replaceOne()`, en lugar de actualizar campos individuales. El método `replaceOne()` sobrescribe todo el documento y conserva únicamente el campo `_id` del original. Si varios documentos coinciden con los criterios del filtro, solo se reemplaza el primer documento encontrado.

```
Document newDocument = new Document()
                .append("restaurantId", "REST-0Y9GL0")
                .append("name", "Bhiryani Adda")
                .append("cuisine", "Indian")
                .append("rating", new Document()
                        .append("average", 4.8)
```

```
                        .append("totalReviews", 267))
                .append("features", Arrays.asList("Outdoor Seating", "Live Music"));

UpdateResult result = collection.replaceOne(
                    Filters.eq("restaurantId", "REST-0Y9GL0"),
                    newDocument);
System.out.printf("Modified %d document%n", result.getModifiedCount());
```

Actualización de documentos múltiples

Hay dos formas de actualizar varios documentos de una colección de forma simultánea. Puede utilizar el método de `updateMany()` o usar el `UpdateManyModel` con el método `bulkWrite()`. El método `updateMany()` utiliza un parámetro de filtro para seleccionar los documentos que se van a actualizar, el parámetro `Update` para identificar los campos que se van a actualizar y un parámetro `UpdateOptions` opcional para especificar las opciones de actualización.

El siguiente ejemplo de código demuestra el uso del método `updateMany()`:

```
Bson filter = Filters.and(
    Filters.in("features", Arrays.asList("Private Dining")),
    Filters.eq("cuisine", "Thai"));
UpdateResult result1 = collection.updateMany(filter, Updates.set("priceRange", "$$$"));
```

El siguiente ejemplo de código demuestra el método de `bulkWrite()` con la misma actualización:

```
BulkWriteOptions options = new BulkWriteOptions().ordered(false);
List < WriteModel < Document >> updates = new ArrayList < > ();
Bson filter = Filters.and(
    Filters.in("features", Arrays.asList("Private Dining")),
    Filters.eq("cuisine", "Indian"));
Bson updateField = Updates.set("priceRange", "$$$");
updates.add(new UpdateManyModel < > (filter, updateField));
BulkWriteResult result = collection.bulkWrite(updates, options);
System.out.printf("Modified %d document%n", result.getModifiedCount());
```

Eliminación de documentos de una colección de DocumentDB

El controlador Java de MongoDB ofrece `deleteOne()` para eliminar un solo documento y `deleteMany()` para eliminar varios documentos que coincidan con criterios específicos. Al igual que la actualización, la operación de eliminación también se puede utilizar con el método

`bulkWrite()`. Ambos `deleteOne()` y `deleteMany()` devuelven un objeto `DeleteResult` que proporciona información sobre el resultado de la operación, incluido el recuento de documentos eliminados. A continuación, se muestra un ejemplo de cómo usar `deleteMany()` para eliminar varios documentos:

```
Bson filter = Filters.and(
    Filters.eq("cuisine", "Thai"),
    Filters.lt("rating.totalReviews", 50));
DeleteResult result = collection.deleteMany(filter);
System.out.printf("Deleted %d document%n", result.getDeletedCount());
```

Gestión de errores con lógica de reintento

Una estrategia sólida de gestión de errores con Amazon DocumentDB debería incluir la categorización de los errores en reintentables (como tiempos de espera de la red o problemas de conexión) y no reintentables (como errores de autenticación o consultas no válidas). En el caso de los errores de operación debidos a errores que deben reintentarse, se debe implementar un intervalo de tiempo entre cada reintento, así como un máximo de reintentos. Las operaciones CRUD deben realizarse en un bloque try-catch que capture `MongoException` y sus subclases. Además, debe incluir la supervisión y el registro de los errores para garantizar la visibilidad operativa. El siguiente es un ejemplo de código que muestra cómo implementar la gestión de errores de reintentos:

```
int MAX_RETRIES = 3;
int INITIAL_DELAY_MS = 1000;
int retryCount = 0;

while (true) {
    try {
        crud_operation(); //perform crud that will throw MongoException or one of its
 subclass
        break;
    } catch (MongoException e) {
        if (retryCount < MAX_RETRIES) {
            retryCount++;
            long delayMs = INITIAL_DELAY_MS * (long) Math.pow(2, retryCount - 1);
            try {
                TimeUnit.MILLISECONDS.sleep(delayMs);
            } catch (InterruptedException t) {
                Thread.currentThread().interrupt();
                throw new RuntimeException("Retry interrupted", t);
            }
```

```
            continue;
        } else
            throw new RuntimeException("Crud operation failed", e);
    }
}
```

Administración de índices en Amazon DocumentDB con Java

Los índices permiten una recuperación eficaz de los datos de una colección de Amazon DocumentDB. Sin índices, DocumentDB debe digitalizar todos los documentos de la colección para obtener resultados que satisfagan una consulta determinada. En este tema se proporciona información sobre cómo crear, eliminar y enumerar índices mediante los controladores Java de MongoDB. También se explica cómo determinar si se está utilizando un índice específico en la consulta y cómo hacer sugerencias a Amazon DocumentDB para que utilice un índice específico.

Temas

- Creación de índices con Java
- Eliminar índices
- Determinación de la selección del índice y proporción de una sugerencia sobre el índice

Amazon DocumentDB admite muchos tipos de índices. Para obtener una descripción general integral de todos los índices compatibles, consulte esta entrada del blog.

Creación de índices con Java

Existen dos mecanismos para crear índices en Amazon DocumentDB con controladores Java de MongoDB: mediante `runCommand()`, y mediante el método `createIndex()` para un índice único o el método `createIndexes()` para varios índices. Uno de los motivos para utilizar los métodos `createIndex()` y `createIndexes()` es que permiten gestionar mejor los errores, ya que detecta errores específicos relacionados con la creación de índices. Otra razón para usar estos métodos en lugar de `runCommand()` es que el controlador Java de MongDB proporciona un amplio conjunto de clases admitidas para la creación y manipulación de índices. Tenga en cuenta que estas clases admitidas pueden utilizarse solamente cuando use los métodos `createIndex()` o `createIndexes()`. Hay tres clases admitidas:

- **`Indexes`**: esta clase sirve como clase de utilidad y ofrece métodos de fábrica estáticos para crear varios tipos de índices. Simplifica el proceso de creación de definiciones de índices complejas y se suele usar junto con otras clases relacionadas con los índices.

- **`IndexModel`**: se trata de una clase fundamental que condensa tanto la definición de las claves de índice como sus opciones. Representa una especificación de índice completa, que combina qué indexar (las claves) con cómo indexar (las opciones). Esta clase es particularmente útil cuando se crean varios índices simultáneamente, ya que permite definir un conjunto de especificaciones de índices que se pueden pasar al método `createIndexes()`.
- **`IndexOptions`**: se trata de una clase de configuración completa que proporciona un amplio conjunto de métodos para personalizar el comportamiento de los índices. Incluye ajustes para índices únicos, índices dispersos, tiempo de caducidad (TTL) y expresiones de filtrado parcial. Mediante el encadenamiento de métodos, puede configurar varias opciones, como la creación de índices en segundo plano y las restricciones únicas.

Creación de un índice único

En este ejemplo se muestra cómo crear un índice único con el método `createIndex()` en segundo plano. Para entender la creación de índices en segundo plano y en primer plano, consulte Tipos de creación de índices. El siguiente ejemplo de código usa `IndexOptions` para crear un índice único con el nombre «unique_restaurantId_idx» en segundo plano. A continuación, este objeto `IndexOptions` se pasa al método `createIndex()`.

```
collection.createIndex(
    Indexes.ascending("restaurantId"),
    new IndexOptions()
        .unique(true)
        .name("unique_restaurantId_idx")
        .background(true));
```

Creación de índices múltiples

En este ejemplo, se crean índices múltiples mediante el método `createIndexes()`. Primero crea la opción para cada índice mediante el objeto de `IndexModel` y, a continuación, pasa una lista de objetos de `IndexModel` al método `createIndexes()`. En el siguiente ejemplo de código se muestra cómo crear un índice compuesto mediante la clase de utilidad `Indexes`. Esta clase también se usa para especificar si desea crear un índice con un orden de clasificación ascendente o descendente. Tras crear índices múltiples, llama al método `listIndexes()` para verificar la creación del índice.

```
// Single Field Index on cuisine
IndexModel singleIndex = new IndexModel(
```

```
    Indexes.ascending("cuisine"),
    new IndexOptions().name("cuisine_idx"));

// Compound Index
IndexModel compoundIndex = new IndexModel(
    Indexes.compoundIndex(
        Indexes.ascending("address.state"),
        Indexes.ascending("priceRange")),
    new IndexOptions().name("location_price_idx"));

// Build a list of IndexModel for the indexes
List < IndexModel > indexes = Arrays.asList(
    singleIndex,
    compoundIndex
);

collection.createIndexes(indexes);

// Verify created indexes
collection.listIndexes().forEach(index - > System.out.println("Created index: " +
 index.toJson()));
```

Creación de índices dispersos y parciales

En este ejemplo se muestra la creación de un índice disperso y uno parcial mediante la creación de un `IndexModel` para cada tipo de índice.

```
// Sparse Index Model, this will identify only those documents that have a
// michelin star rating
IndexModel sparseIndex = new IndexModel(
    Indexes.ascending("michelin.star"),
    new IndexOptions()
    .name("michelin_sparse_idx")
    .sparse(true));

// Partial Index Model where the restaurant is active and has a rating of 4 and above
IndexModel partialIndex = new IndexModel(
    Indexes.ascending("rating.average"),
    new IndexOptions()
    .name("high_rated_active_idx")
    .partialFilterExpression(
        Filters.and(
            Filters.eq("isActive", true),
```

```
            Filters.gte("rating.average", 4.0))));
```

Creación de un índice de texto

En este ejemplo se muestra cómo crear un índice de texto. Solo se permite un índice de texto en una colección, pero ese índice de texto puede ser un índice compuesto que abarque campos múltiples. Cuando usa varios campos en el índice de texto, también puede asignar pesos a cada uno de los campos del índice. Amazon DocumentDB no admite los índices de texto en campos de matriz y, aunque puede utilizar hasta 30 campos en el índice de texto compuesto, solo se puede asignar un peso a tres campos.

```
IndexModel textIndex = new IndexModel(
    new Document()
    .append("name", "text")
    .append("description", "text")
    .append("cuisine", "text"),
    new IndexOptions()
    .name("restaurant_text_idx")
    .weights(new Document()
        .append("name", 10) // Restaurant name gets highest weight
        .append("description", 5) // Description get medium weight
        .append("cuisine", 2) // Cuisine type gets low weight
    ));

collection.createIndex(textIndex.getKeys(), textIndex.getOptions());
```

Creación de un índice mediante el **`runCommand()`**

Amazon DocumentDB admite la creación de índices en paralelo para reducir el tiempo que se tarda en crear índices. La indexación paralela utiliza varios procesos de trabajo simultáneos. La cantidad predeterminada de procesos de trabajo que se utilizan para la creación de índices son dos. Esta entrada del blog ofrece una discusión en profundidad sobre la indexación en paralelo. Actualmente, los controladores Java de MongDB no permiten especificar la opción de proceso de trabajo cuando se utiliza `createIndex()` o `createIndexes()` y, por lo tanto, la única forma de especificar los procesos de trabajo es mediante el `runCommand`. El siguiente ejemplo de código muestra cómo usar `runCommand` para crear un índice que aumente el número de procesos de trabajo a cuatro:

```
Document command = new Document("createIndexes", "Restaurants")
    .append("indexes", Arrays.asList(
        new Document("key", new Document("name", 1))
        .append("name", "restaurant_name_idx")
```

```
        .append("workers", 4) // Specify number of workers
    ));

Document commendResult = connectedDB.runCommand(command);
```

Eliminar índices

El controlador Java de MongoDB proporciona varios métodos para eliminar índices, ya que se adapta a diferentes situaciones y a sus preferencias. Puede eliminar los índices por nombre, por especificación de clave o eliminar todos los índices a la vez. Los métodos `dropIndex()` y `dropIndexes()` pueden invocarse en un objeto de colección para eliminar un índice. Cuando elimina un índice por nombre, debe asegurarse de que se use el nombre de índice correcto, lo que puede no ser siempre intuitivo, especialmente para los índices compuestos o generados de forma automática. Si intenta eliminar un índice inexistente, se obtendrá una `MongoCommandException`. El índice `default _id` no se puede eliminar, ya que garantiza la exclusividad del documento dentro de la colección.

En el siguiente ejemplo de código se muestra cómo eliminar un índice con el nombre del campo donde se creó el índice o mediante la eliminación de todos los índices:

```
String indexName = "unique_restaurantId_idx";
Document keys = new Document("cuisine", 1);
// Drop index by name
collection.dropIndex(indexName);

// Drop index by keys
collection.dropIndex(keys);

// Drop all indexes
collection.dropIndexes();
```

Cuando borra índices con claves múltiples, asegúrese de que haya un índice compuesto que contenga todas las claves especificadas y de que el orden de las claves sea correcto. El código de ejemplo de creación del índice anterior muestra una clave compuesta sobre «cocina» y características. Si intenta eliminar esa clave compuesta pero el orden no es el que se utilizó para la creación, se produce MongoCommnadException el siguiente error:

```
Document keys = new Document("features", 1)
    .append("cuisine", 1);
try {
    // Drop index by keys
```

```
    collection.dropIndex(keys);
    System.out.println("Successfully dropped index with keys: " + keys.toJson());

} catch (MongoCommandException commErr) {
    System.out.println("Error dropping index: " + commErr.getErrorMessage());
    throw new RuntimeException("MongoCommandException was thrown while dropping index",
 commErr);
}
```

Se muestra el siguiente error:

```
Error dropping index: Cannot drop index: index not found.
Tests run: 3, Failures: 1, Errors: 0, Skipped: 0, Time elapsed: 0.819 sec <<< FAILURE!
com.amazon.docdb.guide.DocDBGuideTest.testindexGuide()  Time elapsed: 0.817 sec  <<<
 FAILURE!
org.opentest4j.AssertionFailedError: Unexpected exception thrown:
 java.lang.RuntimeException: MongoCommandException was thrown while dropping index
```

Determinación de la selección del índice y proporción de una sugerencia sobre el índice

Trabajar con la funcionalidad de explicación de Amazon DocumentDB es fundamental para comprender el rendimiento de las consultas y el uso de los índices. Cuando ejecuta una consulta, puede añadir el método `explain()` para obtener información detallada sobre el plan de consulta, incluidos los índices, si los hubiera, que se están utilizando. El resultado `explain()` proporciona información sobre las etapas de ejecución de la consulta, el número de documentos examinados y el tiempo necesario para cada etapa. Esta información es inestimable para identificar si un índice en particular se está utilizando de manera eficaz o si la consulta podría beneficiarse de una estructura de índice diferente.

El método `explain()` se puede encadenar con el método `find()`. El método `explain()` puede utilizar un enumerador opcional `ExplainVerbosity` que determine el nivel de verbosidad devuelto por `explain()`. En este momento, DocumentDB admite solamente los enumeradores `EXECUTION_STATS` y `QUERY_PLANNER`. En el siguiente ejemplo de código se muestra cómo obtener el planificador de consultas para una consulta específica:

```
// Query we want to analyze
Document query = new Document()
    .append("cuisine", "Thai")
    .append("rating.average", new Document("$gte", 4.0));
```

```
Document allPlansExplain =
 collection.find(query).explain(ExplainVerbosity.QUERY_PLANNER);
System.out.println("All Plans Explain:\n" + allPlansExplain.toJson());
```

Se devuelve el siguiente documento JSON para el nivel de verbosidad del planificador de consultas:

```
{
  "queryPlanner": {
    "plannerVersion": 1,
    "namespace": "ProgGuideData.Restaurants",
    "winningPlan": {
      "stage": "IXSCAN",
      "indexName": "cuisine_idx",
      "direction": "forward"
    }
  },
  "serverInfo": {
    "host": "guidecluster3",
    "port": 27017,
    "version": "5.0.0"
  },
  "ok": 1,
  "operationTime": {
    "$timestamp": {
      "t": 1739221668,
      "i": 1
    }
  }
}
```

Dispone de varias opciones para incitar o forzar a Amazon DocumentDB a utilizar un índice específico. Los métodos `hint()` y `hintString()` le permiten anular el comportamiento de selección de índices predeterminado del optimizador de consultas y especificar explícitamente qué índice debe usarse para una consulta. Si bien el optimizador de consultas de DocumentDB suele ser una buena opción para la selección de índices, hay situaciones en las que forzar la aprobación de un índice específico mediante `hint()` o `hintString()` puede resultar beneficioso, como cuando se trata de datos sesgados o se comprueba el rendimiento de un índice.

El siguiente ejemplo de código fuerza el uso de un índice compuesto «cuisine_features_idx» para la misma consulta que se ejecutó en el código anterior:

```
// Query we want to analyze
```

```
Document query = new Document()
    .append("cuisine", "Thai")
    .append("rating.average", new Document("$gte", 4.0));

List < Document > queryDocs = new ArrayList < > ();
collection.find(query).hintString("cuisine_features_idx").forEach(doc - >
 queryDocs.add(doc));
```

Programación basada en eventos con Amazon DocumentDB y Java

La programación basada en eventos en el contexto de Amazon DocumentDB representa un patrón arquitectónico potente en el que los cambios en la base de datos actúan como los principales generadores de eventos que desencadenan la lógica y los procesos empresariales posteriores. Cuando se insertan, actualizan o eliminan registros en una colección de DocumentDB, estos cambios actúan como eventos que inician automáticamente varios procesos posteriores, notificaciones o tareas de sincronización de datos. Este patrón es particularmente valioso en los sistemas distribuidos modernos, donde aplicaciones o servicios múltiples deben reaccionar a los cambios en los datos en tiempo real. El mecanismo principal de implementación de la programación basada en eventos en DocumentDB es mediante flujos de cambios.

> **Note**
>
> En esta guía se asume que habilitó los flujos de cambios en una colección con la que está trabajando. Consulte Uso de flujos de cambios con Amazon DocumentDB para obtener información sobre cómo habilitar los flujos de cambios en la colección.

Trabajo con flujos de cambios desde la aplicación Java

El método `watch()` del controlador Java de MongoDB es el mecanismo principal para supervisar los cambios de datos en tiempo real en Amazon DocumentDB. Los objetos `MongoClient`, `MongoDatabase` y `MongoCollection` pueden llamar al método `watch()`.

El método `watch()` devuelve una instancia de `ChangeStreamIterable` que admite varias opciones de configuración, entre las que se incluyen la búsqueda completa de actualizaciones en los documentos, el suministro de tokens de reanudación y una marca de tiempo para garantizar la fiabilidad, y las etapas de agregación de canalizaciones para filtrar los cambios.

`ChangeStreamIterable` implementa la interfaz básica de Java `Iterable` y puede usarse con `forEach()`. Para capturar eventos mediante `forEach()`, transfiera una función de devolución de

llamada a `forEach()` que procese el evento cambiado. En el siguiente fragmento de código se muestra cómo abrir un flujo de cambios en una colección para iniciar la supervisión de eventos de cambio:

```
ChangeStreamIterable < Document > iterator = collection.watch();
iterator.forEach(event - > {
    System.out.println("Received a change: " + event);
});
```

Otra forma de recorrer todos los eventos de cambio consiste en abrir un cursor que mantenga una conexión con el clúster y reciba continuamente nuevos eventos de cambio a medida que se producen. Para obtener un cursor de flujo de cambios, utilice el método `cursor()` del objeto `ChangeStreamIterable`. En el siguiente ejemplo de código se muestra cómo supervisar eventos de cambio con el cursor:

```
try (MongoChangeStreamCursor < ChangeStreamDocument < Document >> cursor =
 collection.watch().cursor()) {
    System.out.println(cursor.tryNext());
}
```

Como práctica recomendada, puede crearla `MongoChangeStreamCursor`en una try-with-resource sentencia o cerrar el cursor manualmente. Si se llama al método `cursor()` en `ChangeStreamIterable`, se devuelve un `MongoChangeStreamCursor` creado sobre un objeto de `ChangeStreamDocument`.

La clase `ChangeStreamDocument` es un componente crucial que representa los eventos de cambio individuales en el flujo. Contiene información detallada sobre cada modificación, incluido el tipo de operación (insertar, actualizar, eliminar, reemplazar), la clave del documento, la información del espacio de nombres y el contenido completo del documento, cuando esté disponible. La clase proporciona métodos para acceder a varios aspectos del evento de cambio, como `getOperationType()` para determinar el tipo de cambio, `getFullDocument()` para acceder al estado completo del documento y `getDocumentKey()` para identificar el documento modificado.

El objeto `ChangeStreamDocument` proporciona dos datos importantes: un token de reanudación y la hora del evento de cambio.

Los tokens de reanudación y las operaciones basadas en el tiempo en los flujos de cambios de DocumentDB proporcionan mecanismos cruciales para mantener la continuidad y administrar el

acceso a los datos históricos. Un token de reanudación es un identificador único que se genera para cada evento de cambio y sirve como marcador que permite que las aplicaciones reinicien el procesamiento del flujo de cambios desde un punto específico tras una desconexión o un fallo. Cuando se crea un cursor de flujo de cambios, se puede usar un token de reanudación previamente almacenado mediante la opción `resumeAfter()`, lo que permite que el flujo continúe desde donde dejó en lugar de empezar desde el principio o perder los eventos.

Las operaciones basadas en el tiempo en los flujos de cambios ofrecen diferentes enfoques para gestionar el punto de partida de la supervisión de los eventos de cambio. La opción `startAtOperationTime()` le permite empezar a observar los cambios que ocurrieron en una marca de tiempo específica o después de esta. Estas funciones basadas en el tiempo son particularmente valiosas en escenarios que requieren el procesamiento, la point-in-time recuperación o la sincronización de datos históricos entre sistemas.

El siguiente ejemplo de código recupera el evento asociado al documento de inserción, captura su token de reanudación y, a continuación, proporciona ese token para empezar a supervisar los eventos posteriores al evento de inserción. El evento se asocia al evento de actualización y, a continuación, obtiene la hora del clúster en que se produjo la actualización y utiliza esa marca de tiempo como punto de partida para el procesamiento posterior.

```
BsonDocument resumeToken;
BsonTimestamp resumeTime;

try (MongoChangeStreamCursor < ChangeStreamDocument < Document >> cursor =
 collection.watch().cursor()) {
    System.out.println("****************** Insert Document ******************");
    ChangeStreamDocument < Document > insertChange = cursor.tryNext();
    resumeToken = insertChange.getResumeToken();
    printJson(cursor.tryNext());
}
try (MongoChangeStreamCursor < ChangeStreamDocument < Document >> cursor =
 collection.watch()
    .resumeAfter(resumeToken)
    .cursor()) {
    System.out.println("****************** Update Document ******************");
    ChangeStreamDocument < Document > insertChange = cursor.tryNext();
    resumeTime = insertChange.getClusterTime();
    printJson(cursor.tryNext());
}
try (MongoChangeStreamCursor < ChangeStreamDocument < Document >> cursor =
 collection.watch()
```

```
    .startAtOperationTime(resumeTime)
    .cursor()) {
    System.out.println("****************** Delete Document ******************");
    printJson(cursor.tryNext());
  }
```

De manera predeterminada, el evento de cambio de actualización no incluye el documento completo, sino tan solo los cambios realizados. Si necesita acceder al documento completo que se actualizó, puede llamar al método `fullDocument()` en el objeto `ChangeStreamIterable`. Tenga en cuenta que, cuando solicita que se devuelva un documento completo para un evento de actualización, se devolverá el documento que existía en el momento en que se realizó la llamada al flujo de cambios.

Este método toma un enumerador `FullDocument` como parámetro. Actualmente, Amazon DocumentDB admite solamente valores DEFAULT y `UPDATE_LOOKUP`. El siguiente fragmento de código muestra cómo solicitar el documento completo para los eventos de actualización cuando empieza a observar los cambios:

```
try (MongoChangeStreamCursor < ChangeStreamDocument < Document >> cursor =
 collection.watch().fullDocument(FullDocument.UPDATE_LOOKUP).cursor())
```

Cómo utilizar la validación de esquemas JSON

Con el operador de consulta de evaluación de `$jsonSchema`, puede validar los documentos que se están insertando en sus colecciones.

Temas

- Cómo crear y utilizar la validación de esquemas JSON
- Palabras clave compatibles
- bypassDocumentValidation
- Limitaciones

Cómo crear y utilizar la validación de esquemas JSON

Cómo crear una colección con validación de esquemas

Puede crear una colección con reglas de operación y validación de `createCollection`. Estas reglas de validación se aplican al insertar o actualizar documentos de Amazon DocumentDB. En el siguiente ejemplo de código se muestran las reglas de validación para un conjunto de empleados:

```
db.createCollection("employees", {
   "validator": {
      "$jsonSchema": {
         "bsonType": "object",
         "title": "employee validation",
         "required": [ "name", "employeeId"],
         "properties": {
            "name": {
                  "bsonType": "object",
                  "properties": {
                     "firstName": {
                        "bsonType": ["string"]
                     },
                     "lastName": {
                        "bsonType": ["string"]
                     }
                  },
                  "additionalProperties" : false
            },
            "employeeId": {
               "bsonType": "string",
               "description": "Unique Identifier for employee"
            },
             "salary": {
               "bsonType": "double"
            },
            "age": {
               "bsonType": "number"
            }
         },
         "additionalProperties" : true
      }
   },
   "validationLevel": "strict", "validationAction": "error"
} )
```

Cómo insertar un documento válido

En el siguiente ejemplo, se insertan documentos que cumplen con las reglas de validación de esquemas anteriores:

```
db.employees.insert({"name" : { "firstName" : "Carol" , "lastName" : "Smith"},
 "employeeId": "c720a" , "salary": 1000.0 })
```

```
db.employees.insert({ "name" : { "firstName" : "William", "lastName" : "Taylor" },
 "employeeId" : "c721a", "age" : 24})
```

Cómo insertar un documento no válido

En el siguiente ejemplo, se insertan documentos que no cumplen con las reglas de validación de esquemas anteriores. En este ejemplo, el valor employeeId no es una cadena:

```
db.employees.insert({
    "name" : { "firstName" : "Carol" , "lastName" : "Smith"},
    "employeeId": 720 ,
    "salary": 1000.0
})
```

En este ejemplo, se muestra una sintaxis incorrecta en el documento.

Modificación de una colección

El comando `collMod` se utiliza para añadir o modificar las reglas de validación de la colección existente. En el siguiente ejemplo se añade un campo de salario a la lista de campos obligatorios:

```
db.runCommand({"collMod" : "employees",
   "validator": {
      "$jsonSchema": {
         "bsonType": "object",
         "title": "employee validation",
         "required": [ "name", "employeeId", "salary"],
         "properties": {
            "name": {
                  "bsonType": "object",
                  "properties": {
                     "firstName": {
                        "bsonType": ["string"]
                     },
                     "lastName": {
                        "bsonType": ["string"]
                     }
                  },
                  "additionalProperties" : false
            },
            "employeeId": {
               "bsonType": "string",
```

```
               "description": "Unique Identifier for employee"
            },
             "salary": {
               "bsonType": "double"
            },
            "age": {
               "bsonType": "number"
            }
         },
         "additionalProperties" : true
      }
   }
} )
```

Cómo abordar los documentos añadidos antes de que se cambiaran las reglas de validación

Para abordar los documentos que se añadieron a su colección antes de que se cambiaran las reglas de validación, utilice los siguientes modificadores de `validationLevel`:

- estricto: aplica reglas de validación a todas las inserciones y actualizaciones.
- moderado: aplica reglas de validación a los documentos válidos existentes. Durante las actualizaciones, no se comprueban los documentos no válidos existentes.

En el siguiente ejemplo, tras actualizar las reglas de validación de la colección denominada “empleados”, el campo de salario es obligatorio. No se podrá actualizar el siguiente documento:

```
db.runCommand({
    update: "employees",
    updates: [{
        q: { "employeeId": "c721a" },
        u: { age: 25 , salary : 1000},
        upsert: true }]
})
```

Amazon DocumentDB devuelve el siguiente resultado:

```
{
"n" : 0,
    "nModified" : 0,
    "writeErrors" : [
        {
```

```
"index" : 0,
            "code" : 121,
            "errmsg" : "Document failed validation"
        }
    ],
    "ok" : 1,
    "operationTime" : Timestamp(1234567890, 1)
}
```

Si se actualiza el nivel de validación a `moderate`, se permitirá actualizar el documento anterior correctamente:

```
db.runCommand({
    "collMod" : "employees",
    validationLevel : "moderate"
})

db.runCommand({
    update: "employees",
    updates: [{
        q: { "employeeId": "c721a" },
        u: { age: 25 , salary : 1000},
        upsert: true }]
})
```

Amazon DocumentDB devuelve el siguiente resultado:

```
{
"n" : 1,
    "nModified" : 1,
    "ok" : 1,
    "operationTime" : Timestamp(1234567890, 1)
}
```

Recuperación de documentos con el $jsonSchema

El operador de `$jsonSchema` se puede utilizar como filtro para consultar documentos que coincidan con el esquema JSON. Se trata de un operador de nivel superior que puede estar presente en los documentos de filtro como campo de nivel superior o utilizarse con operadores de consulta como `$and`, `$or` y `$nor`. En los siguientes ejemplos se muestra el uso de $jsonSchema como filtro individual y con otros operadores de filtro:

Documento insertado en una colección de “empleado”:

```
{ "name" : { "firstName" : "Carol", "lastName" : "Smith" }, "employeeId" : "c720a",
 "salary" : 1000 }
{ "name" : { "firstName" : "Emily", "lastName" : "Brown" }, "employeeId" : "c720b",
 "age" : 25, "salary" : 1050.2 }
{ "name" : { "firstName" : "William", "lastName" : "Taylor" }, "employeeId" : "c721a",
 "age" : 24, "salary" : 1400.5 }
{ "name" : { "firstName" : "Jane", "lastName" : "Doe" }, "employeeId" : "c721a",
 "salary" : 1300 }
```

Colección filtrada únicamente con el operador de `$jsonSchema`:

```
db.employees.find({
       $jsonSchema: { required: ["age"] } })
```

Amazon DocumentDB devuelve el siguiente resultado:

```
{ "_id" : ObjectId("64e5f91c6218c620cf0e8f8b"), "name" : { "firstName" : "Emily",
 "lastName" : "Brown" }, "employeeId" : "c720b", "age" : 25, "salary" : 1050.2 }
{ "_id" : ObjectId("64e5f94e6218c620cf0e8f8c"), "name" : { "firstName" : "William",
 "lastName" : "Taylor" }, "employeeId" : "c721a", "age" : 24, "salary" : 1400.5 }
```

Colección filtrada con el operador de `$jsonSchema` y otro operador:

```
db.employees.find({
       $or: [{ $jsonSchema: { required: ["age", "name"]}},
            { salary: { $lte:1000}}]});
```

Amazon DocumentDB devuelve el siguiente resultado:

```
{ "_id" : ObjectId("64e5f8886218c620cf0e8f8a"), "name" : { "firstName" : "Carol",
 "lastName" : "Smith" }, "employeeId" : "c720a", "salary" : 1000 }
{ "_id" : ObjectId("64e5f91c6218c620cf0e8f8b"), "name" : { "firstName" : "Emily",
 "lastName" : "Brown" }, "employeeId" : "c720b", "age" : 25, "salary" : 1050.2 }
{ "_id" : ObjectId("64e5f94e6218c620cf0e8f8c"), "name" : { "firstName" : "William",
 "lastName" : "Taylor" }, "employeeId" : "c721a", "age" : 24, "salary" : 1400.5 }
```

Colección filtrada con el operador de `$jsonSchema` y con `$match` en el filtro de agregación:

```
db.employees.aggregate(
    [{ $match: {
        $jsonSchema: {
            required: ["name", "employeeId"],
            properties: {"salary" :{"bsonType": "double"}}
        }
       }
    }]
)
```

Amazon DocumentDB devuelve el siguiente resultado:

```
{
"_id" : ObjectId("64e5f8886218c620cf0e8f8a"),
 "name" : { "firstName" : "Carol", "lastName" : "Smith" },
"employeeId" : "c720a",
"salary" : 1000
}
{
"_id" : ObjectId("64e5f91c6218c620cf0e8f8b"),
"name" : { "firstName" : "Emily", "lastName" : "Brown" },
"employeeId" : "c720b",
"age" : 25,
"salary" : 1050.2
}
{
"_id" : ObjectId("64e5f94e6218c620cf0e8f8c"),
"name" : { "firstName" : "William", "lastName" : "Taylor" },
"employeeId" : "c721a",
"age" : 24,
"salary" : 1400.5
}
{
"_id" : ObjectId("64e5f9786218c620cf0e8f8d"),
"name" : { "firstName" : "Jane", "lastName" : "Doe" },
"employeeId" : "c721a",
"salary" : 1300
}
```

Cómo visualizar las reglas de validación existentes

Para ver las reglas de validación existentes en una colección, utilice:

```
db.runCommand({
    listCollections: 1,
    filter: { name: 'employees' }
})
```

Amazon DocumentDB devuelve el siguiente resultado:

```
{
    "waitedMS" : NumberLong(0),
    "cursor" : {
        "firstBatch" : [
            {
                "name" : "employees",
                "type" : "collection",
                "options" : {
                    "autoIndexId" : true,
                    "capped" : false,
                    "validator" : {
                        "$jsonSchema" : {
                            "bsonType" : "object",
                            "title" : "employee validation",
                            "required" : [
                                "name",
                                "employeeId",
                                "salary"
                            ],
                            "properties" : {
                                "name" : {
                                    "bsonType" : "object",
                                    "properties" : {
                                        "firstName" : {
                                            "bsonType" : [
                                                "string"
                                            ]
                                        },
                                        "lastName" : {
                                            "bsonType" : [
                                                "string"
                                            ]
                                        }
                                    },
                                    "additionalProperties" : false
                                },
```

```
                                "employeeId" : {
                                    "bsonType" : "string",
                                    "description" : "Unique Identifier for employee"
                                },
                                "salary" : {
                                    "bsonType" : "double"
                                },
                                "age" : {
                                    "bsonType" : "number"
                                }
                            },
                            "additionalProperties" : true
                        }
                    },
                    "validationLevel" : "moderate",
                    "validationAction" : "error"
                },
                "info" : {
                    "readOnly" : false
                },
                "idIndex" : {
                    "v" : 2,
                    "key" : {
                        "_id" : 1
                    },
                    "name" : "_id_",
                    "ns" : "test.employees"
                }
            }
        ],
        "id" : NumberLong(0),
        "ns" : "test.$cmd.listCollections"
    },
    "ok" : 1,
    "operationTime" : Timestamp(1692788937, 1)
}
```

Amazon DocumentDB también conserva las reglas de validación en la etapa de agregación `$out`.

Palabras clave compatibles

Los comandos `create` y `collMod` admiten los siguientes campos:

- **`Validator`**: admite el operador `$jsonSchema`.

- **`ValidationLevel`**: admite los valores `off`, `strict` y `moderate`.
- **`ValidationAction`**: admite el valor `error`.

El operador $jsonSchema admite las siguientes palabras clave:

- `additionalItems`
- `additionalProperties`
- `allOf`
- `anyOf`
- `bsonType`
- `dependencies`
- `description`
- `enum`
- `exclusiveMaximum`
- `exclusiveMinimum`
- `items`
- `maximum`
- `minimum`
- `maxItems`
- `minItems`
- `maxLength`
- `minLength`
- `maxProperties`
- `minProperties`
- `multipleOf`
- `not`
- `oneOf`
- `pattern`
- `patternProperties`
- `properties`
- `required`

- `title`
- `type`
- `uniqueItems`

bypassDocumentValidation

Amazon DocumentDB admite `bypassDocumentValidation` para los siguientes comandos y métodos:

- `insert`
- `update`
- `findAndModify`
- Etapa `$out` en el comando `aggregate` y en el método `db.collection.aggregate()`

Amazon DocumentDB no admite los siguientes comandos para `bypassDocumentValidation`:

- `$merge` en el comando `aggregate` y en el método `db.collection.aggregate()`
- Comando `mapReduce` y método `db.collection.mapReduce()`
- `applyOps`Comando de la

Limitaciones

Las siguientes limitaciones se aplican a la validación de `$jsonSchema`:

- Amazon DocumentDB devuelve el error “No se pudo validar el documento” cuando una operación no cumple con la regla de validación.
- Los clústeres elásticos de Amazon DocumentDB no admiten `$jsonSchema`.

Cuotas y límites de Amazon DocumentDB

En este tema se describen las cuotas, los límites de recursos y las restricciones de nomenclatura para Amazon DocumentDB (compatible con MongoDB).

Para determinadas funciones de administración, Amazon DocumentDB utiliza tecnología operativa que se comparte con Amazon Relational Database Service (Amazon RDS) y Amazon Neptune.

Temas

- Tipos de instancias admitidas
- Regiones admitidas
- Cuotas regionales
- Límites de agregación
- Límites de los clústeres
- Límites de instancias
- Restricciones en la nomenclatura
- Restricciones de TTL
- Límites de clústeres elásticos
- Límites de partición de clústeres elásticos
- Límites de CPU, memoria, conexión y cursor de los clústeres elásticos por partición

Tipos de instancias admitidas

Amazon DocumentDB admite instancias bajo demanda y los siguientes tipos de instancias:

- NVMe-respaldado:
  - Tipos de instancias R6GD: `db.r6gd.xlarge`, `db.r6gd.2xlarge`, `db.r6gd.4xlarge`, `db.r6gd.8xlarge`, `db.r6gd.12xlarge`, `db.r6gd.16xlarge`.
- Optimizada para memoria:
  - Tipos de instancias R6G: `db.r6g.large`, `db.r6g.2xlarge`, `db.r6g.4xlarge`, `db.r6g.8xlarge`, `db.r6g.12xlarge`, `db.r6g.16xlarge`.
  - Tipos de instancias de R5: `db.r5.large`, `db.r5.2xlarge`, `db.r5.4xlarge`, `db.r5.8xlarge`, `db.r5.12xlarge`, `db.r5.16xlarge` `db.r5.24xlarge`.

  - Tipos de instancias de R4: `db.r4.large`, `db.r4.2xlarge`, `db.r4.4xlarge`, `db.r4.8xlarge`, `db.r4.16xlarge`.
- Rendimiento ampliable:
  - Tipos de instancias T4G: `db.t4g.medium`.
  - Tipo de instancias T3: `db.t3.medium`.

Para obtener más información sobre los tipos de instancias admitidos y sus especificaciones, consulte Especificaciones de clases de instancias.

Regiones admitidas

Amazon DocumentDB está disponible en las siguientes regiones: AWS

Nombre de la región	Region	Zonas de disponibilidad (cálculo)
Este de EE. UU. (Ohio)	`us-east-2`	3
Este de EE. UU. (Norte de Virginia)	`us-east-1`	6
Oeste de EE. UU. (Oregón)	`us-west-2`	4
África (Ciudad del Cabo)	`af-south-1`	3
América del Sur (São Paulo)	`sa-east-1`	3
Asia-Pacífico (Hong Kong)	`ap-east-1`	3
Asia-Pacífico (Hyderabad)	`ap-south-2`	3
Asia-Pacífico (Malasia)	`ap-southeast-5`	3
Asia-Pacífico (Mumbai)	`ap-south-1`	3
Asia-Pacífico (Osaka)	`ap-northeast-3`	3
Asia-Pacífico (Seúl)	`ap-northeast-2`	4
Asia-Pacífico (Singapur)	`ap-southeast-1`	3

Nombre de la región	Region	Zonas de disponibilidad (cálculo)
Asia-Pacífico (Sídney)	ap-southeast-2	3
Asia-Pacífico (Yakarta)	ap-southeast-3	3
Asia-Pacífico (Tailandia)	ap-southeast-7	3
Asia-Pacífico (Tokio)	ap-northeast-1	3
Canadá (centro)	ca-central-1	3
Región China (Pekín)	cn-north-1	3
China (Ningxia)	cn-northwest-1	3
Europa (Fráncfort)	eu-central-1	3
Europa (Irlanda)	eu-west-1	3
Europa (Londres)	eu-west-2	3
Europa (Milán)	eu-south-1	3
Europa (París)	eu-west-3	3
Europa (España)	eu-south-2	3
Europa (Estocolmo)	eu-north-1	3
México (centro)	mx-central-1	3
Medio Oriente (EAU)	me-central-1	3
Israel (Tel Aviv)	il-central-1	3
AWS GovCloud (EE. UU.-Oeste)	us-gov-west-1	3

Nombre de la región	Region	Zonas de disponibilidad (cálculo)
AWS GovCloud (EEUU-Este)	`us-gov-east-1`	3

Cuotas regionales

Para determinadas funciones de administración, Amazon DocumentDB utiliza tecnología operativa que se comparte con Amazon Relational Database Service (Amazon RDS). La siguiente tabla contiene los límites regionales que comparten entre Amazon DocumentDB y Amazon RDS.

> **Note**
>
> La tecnología compartida de Amazon RDS descrita anteriormente solo se aplica a los clústeres basados en instancias de Amazon DocumentDB. Los clústeres elásticos de Amazon DocumentDB no comparten tecnología con Amazon RDS.

Los siguientes límites se aplican a los clústeres basados en instancias de Amazon DocumentDB y son por cuenta y región. AWS

Recurso	AWS límite predeterminado
Clústeres	40
Grupos de parámetros de clústeres	50
Suscripciones de eventos	20
Instancias	40
Instantáneas de clústeres manuales	100
Réplicas de lectura por clúster	15
Grupos de subredes	50
Subredes por grupo de subredes	20

Recurso	AWS límite predeterminado
Etiquetas por recurso	50
Grupos de seguridad de VPC por instancia	5

Los siguientes límites se aplican a los clústeres elásticos de Amazon DocumentDB y son por AWS cuenta y región.

Recurso	AWS límite predeterminado
Clústeres elásticos	20
vCPU de clústeres elásticos	1024
Instantánea de un clúster elástico manual	20

Puede utilizar Service Quotas para solicitar un aumento de una cuota, si esta es ajustable. Algunas solicitudes se resuelven automáticamente, mientras que otras se envían a Soporte. Puede realizar un seguimiento del estado de una solicitud de aumento de cuota que se envía a Soporte. Las solicitudes para aumentar las Service Quotas no reciben soporte prioritario. Si tiene una solicitud urgente, póngase en contacto con Soporte. Para obtener más información acerca de las Service Quotas, consulte What Is Service Quotas?

Para solicitar un aumento de cuota de Amazon DocumentDB:

1. Abra la consola de Service Quotas en https://console.aws.amazon.com/servicequotas y, si es necesario, inicie sesión.
2. En el panel de navegación, elija Servicios de AWS .
3. Seleccione clúster elástico de Amazon DocumentDB o Amazon DocumentDB (compatible con MongoDB) en la lista o escriba cualquiera de estas dos opciones en el campo de búsqueda.
4. Si la cuota es ajustable, puede seleccionar su botón de opción o su nombre y, a continuación, seleccionar Request quota increase (Solicitar aumento de cuota) en la parte superior derecha de la página.
5. En Change quota value (Cambiar valor de cuota), introduzca el nuevo valor. El nuevo valor debe ser mayor que el valor actual.

6. Seleccione Solicitar. Una vez resuelta la solicitud, Valor de cuota aplicada para la cuota se establece en el nuevo valor.
7. Para ver las solicitudes pendientes o resueltas recientemente, elija Panel en el panel de navegación. Para las solicitudes pendientes, seleccione el estado de la solicitud para abrir la recepción de solicitud. El estado inicial de una solicitud es `Pending`. Cuando el estado cambie a`Quota requested`, verás el número de caso con Soporte. Elija el número de caso para abrir el ticket para su solicitud.

Límites de agregación

En la siguiente tabla se describen los límites de agregación de Amazon DocumentDB.

Recurso	Límite
Número máximo de etapas admitidas	500

Límites de los clústeres

En la tabla siguiente se describen los límites de clúster en función de la instancia de Amazon DocumentDB.

Recurso	Límite
Tamaño del clúster (suma de todas las colecciones e índices)	128 TiB
Tamaño de la colección (la suma de todas las colecciones no puede superar el límite del clúster): no incluye el tamaño del índice	32 TiB
Colecciones por clúster	100 000
Bases de datos por clúster	100 000
Tamaño de la base de datos (la suma de todas las bases de datos no puede superar el límite del clúster)	128 TiB
Profundidad de anidamiento de documentos	200 niveles
Tamaño del documento	16 MiB
Tamaño de clave de índice	2048 bytes
Índices por colección	64
Claves de un índice compuesto	32

Recurso	Límite
Número máximo de operaciones de escritura en un único comando por lotes	100 000
Número de usuarios por clúster	1 000

Límites de instancias

En la tabla siguiente se describen los límites de Amazon DocumentDB por instancia.

Tipo de instancia	Memoria de la instancia (GiB)	Conexiones (todas)	Límite del cursor	Transacciones abiertas	Conexiones (activas)
t3.medium	4	1 000	30	50	102
T4G.medium	4	1 000	30	50	102
R4.large	15.25	1700	450	N/A	1 100
R4.xlarge	30.5	3400	450	N/A	2700
R4.2xlarge	61	6800	450	N/A	4500
R4.4xlarge	122	13600	725	N/A	4500
R4.8xlarge	288	27200	1450	N/A	4500
R4.16xlarge	488	30000	2900	N/A	4500
R5.large	16	3400	450	200	1 100
R5.xlarge	32	7000	450	400	2700
R5.2xlarge	64	14200	450	800	4500
R5.4xlarge	128	28400	760	1600	4500
R5.8xlarge	256	60000	1520	3200	4500
R5.12xlarge	384	60000	2280	4800	4500
R5.16xlarge	512	60000	3040	6400	4500
R5.24xlarge	768	60000	4560	9600	4500
R6G.large*	16	3400	450	200	1 100

Tipo de instancia	Memoria de la instancia (GiB)	Conexiones (todas)	Límite del cursor	Transacciones abiertas	Conexiones (activas)
R6G.xlarge*	32	7000	450	400	2700
R6G.2xlarge*	64	14200	450	800	4500
R6G.4xlarge*	128	28400	760	1600	4500
R6G.8xlarge*	256	60000	1520	3200	4500
R6G.12xlarge*	384	60000	2280	4800	4500
R6G.16xlarge*	512	60000	3040	6400	4500

* Incluido R6GD.

Puede monitorear y emitir alarmas sobre los límites por instancia mediante las siguientes CloudWatch métricas. Para obtener más información sobre las CloudWatch métricas de Amazon DocumentDB, consulte. Supervisión de Amazon DocumentDB con CloudWatch

Recurso	CloudWatch métrica límite	CloudWatch métrica de uso (1 minuto como máximo)	CloudWatch métrica de uso
Memoria de la instancia	-	-	FreeableMemory
Conexiones (todas)	DatabaseConnectionsLimit	DatabaseConnectionsMax	DatabaseConnections
Cursores	DatabaseCursorsLimit	DatabaseCursorsMax	DatabaseCursors
Transacciones	TransactionsOpenLimit	TransactionsOpenMax	TransactionsOpen

Restricciones en la nomenclatura

En la siguiente tabla se describen las restricciones de la nomenclatura en Amazon DocumentDB.

Recurso	Límite predeterminado
Identificador de clúster	• Debe tener [1-63] letras, números o guiones. • El primer carácter debe ser una letra. • No puede terminar con un guion ni contener dos guiones consecutivos. • Debe ser único para todos los clústeres (en Amazon RDS, Amazon Neptune y Amazon DocumentDB) AWS por cuenta y región.
Nombre de la colección: `<col>`	La longitud es [1-57] caracteres.
Nombre de la base de datos: `<db>`	La longitud es [1-63] caracteres.
Nombre completo de la colección: `<db>.<col>`	La longitud es [3-120] caracteres.
Nombre completo del índice: `<db>.<col>$<index>`	La longitud es [6-377] caracteres.
Nombre del índice: `<col>$<index>`	La longitud es [3-255] caracteres.
Identificador de instancia	• Debe tener [1-63] letras, números o guiones • El primer carácter debe ser una letra • No puede terminar por un guion ni contener dos guiones consecutivos

Recurso	Límite predeterminado
	• Debe ser único para todas las instancias (en Amazon RDS, Amazon Neptune y Amazon DocumentDB) AWS por cuenta y región.

Contraseña principal	• La longitud es de [8-100] caracteres ASCII imprimibles.
	• Se puede utilizar cualquier carácter ASCII imprimible, excepto los siguientes:
	  • `/` (barra inclinada)
	  • `"` (comillas dobles)
	  • `@` (símbolo de arroba)

Nombre de usuario principal	• La longitud es de [1-63] caracteres alfanuméricos. • El primer carácter debe ser una letra. • No puede ser una palabra reservada por el motor de base de datos.
Nombre del grupo de parámetros	• La longitud es de [1-255] caracteres alfanuméricos. • El primer carácter debe ser una letra. • No puede terminar con un guion ni contener dos guiones consecutivos.

Restricciones de TTL

Las eliminaciones de un índice de TTL no están garantizadas en un periodo de tiempo específico y se efectúan en la medida que sea posible. Factores como la utilización de recursos de instancia, el tamaño del documento y el rendimiento general pueden afectar la temporización de una eliminación de TTL.

Límites de clústeres elásticos

En la tabla siguiente se describen los límites máximos de clúster de Amazon DocumentDB.

Recurso	Límite
Clústeres elásticos por región	20
vCPU sumada en todos los clústeres elásticos por región	1024
Instantáneas de clúster manuales por región	20
Particiones por clúster	32
Almacenamiento por clúster (cuando los datos se distribuyen uniformemente por la clave de partición)	4 PiB
Conexiones al clúster	El valor inferior de 300 000 o el número de particiones x el límite de conexión asociado a la vCPU por partición
UnSharded tamaño de la colección	32 TiB
Tamaño de la colección con particiones (cuando los datos se distribuyen uniformem ente mediante la clave de partición)	1 PB
Bases de datos por clúster	10 000
UnSharded colecciones por clúster	100 000

Recurso	Límite
Colecciones por clúster con particiones	1 000
Usuarios por clúster	100
Escritura en un único comando por lotes	100 000
Índices por colección	64
Profundidad de anidamiento de documentos	100 niveles
Tamaño del documento	16 MB
Tamaño de clave de índice	2048 bytes
Claves de un índice compuesto	32

Límites de partición de clústeres elásticos

En la tabla siguiente se describen los límites máximos de partición de clústeres elásticos de Amazon DocumentDB.

Recurso	Límite
vCPU por instancia de partición	64
Instancias por partición	16
Almacenamiento por partición	128 TiB
Almacenamiento por colección y por partición	32 TiB

Límites de CPU, memoria, conexión y cursor de los clústeres elásticos por partición

En la siguiente tabla se describen los límites máximos de CPU, memoria, conexión y cursor en las particiones de los clústeres elásticos de Amazon DocumentDB.

v CPUs por fragmento	Memoria de la instancia (GiB)	Límites de conexión	Límite del cursor
2	16	1700	450
4	32	3500	450
8	64	7100	450
16	128	14200	760
32	256	28400	1520
48	384	30000	2280
64	512	30000	3040

Consultas en Amazon DocumentDB

En esta sección se explican todos los aspectos de las consultas con Amazon DocumentDB.

Temas

- Consulta de documentos
- Plan de consulta
- Descripción de los resultados
- Planificador de consultas v2
- Planificador de consultas v3
- Consulta de datos geoespaciales con Amazon DocumentDB
- Índice parcial
- Búsquedas de texto con Amazon DocumentDB

Consulta de documentos

A veces, es posible que tenga que examinar el inventario de su tienda online para que los clientes puedan ver y comprar lo que usted vende. Consultar una colección es relativamente fácil, tanto si desea consultar todos los documentos de la colección como solo aquellos que cumplan un determinado criterio.

Para consultar documentos, utilice la operación `find()`. El comando `find()` tiene un único parámetro de documento que define los criterios que se utilizan al elegir los documentos que se devuelven. El resultado de `find()` es un documento formateado como una sola línea de texto sin saltos de línea. Para formatear el documento resultante para facilitar su lectura, utilice `find().pretty()`. En todos los ejemplos que se muestran en este tema, se utiliza `.pretty()` para formatear la salida.

Los siguientes ejemplos de código utilizan los cuatro documentos que insertó en la colección `example` en los dos ejercicios anteriores: `insertOne()` y `insertMany()` que se encuentran en la sección sobre cómo agregar documentos de Trabajar con documentos.

Temas

- Recuperar todos los documentos de una colección
- Recuperación de documentos que coincidan con un valor de campo

- Recuperación de documentos que coincidan con un documento incrustado
- Recuperación de documentos que coincidan con un valor de campo de un documento incrustado
- Recuperación de documentos que coincidan con una matriz
- Recuperación de documentos que coincidan con un valor de una matriz
- Recuperación de documentos mediante operadores

Recuperar todos los documentos de una colección

Para recuperar todos los documentos de la colección, utilice la operación `find()` con un documento de consulta vacío.

La siguiente consulta devuelve todos los documentos de la colección `example`.

```
db.example.find( {} ).pretty()
```

Recuperación de documentos que coincidan con un valor de campo

Para recuperar todos los documentos que coincidan con un campo y valor, utilice la operación `find()` con un documento de consulta que identifique los campos y valores que desee.

Si se utilizan los documentos anteriores, esta consulta devuelve todos los documentos cuyo campo "Item" contiene "Pen".

```
db.example.find( { "Item": "Pen" } ).pretty()
```

Recuperación de documentos que coincidan con un documento incrustado

Para buscar todos los documentos que coinciden con un documento incrustado, utilice la operación `find()` con un documento de consulta que especifique el nombre del documento incrustado y todos los campos y los valores de ese documento incrustado.

Cuando se buscan coincidencias con un documento incrustado, el documento incrustado del documento debe tener el mismo nombre que en la consulta. Además, los campos y los valores del documento incrustado deben coincidir con la consulta.

La siguiente consulta devuelve únicamente el documento "Poster Paint". Esto se debe a que "Pen" tiene diferentes valores para "`MinOnHand`" y "`OnHand`", y "Spray Paint" tiene un campo más (`OrderQnty`) que el documento de consulta.

```
db.example.find({"Inventory": {
    "OnHand": 47,
    "MinOnHand": 50 } } ).pretty()
```

Recuperación de documentos que coincidan con un valor de campo de un documento incrustado

Para buscar todos los documentos que coinciden con un documento incrustado, utilice la operación `find()` con un documento de consulta que especifique el nombre del documento incrustado y todos los campos y los valores de ese documento incrustado.

Dados los documentos anteriores, la siguiente consulta utiliza la "notación de puntos" para especificar el documento incrustado y los campos de interés. Se devolverá cualquier documento que coincida con ellos, independientemente de los otros campos que puedan existir en el documento incrustado. La consulta devuelve "Poster Paint" y "Spray Paint", ya que ambos coinciden con los campos y los valores especificados.

```
db.example.find({"Inventory.OnHand": 47, "Inventory.MinOnHand": 50 }).pretty()
```

Recuperación de documentos que coincidan con una matriz

Para buscar todos los documentos que coincidan con una matriz, utilice la operación `find()` con el nombre de la matriz que le interese y todos los valores de esa matriz. La consulta devuelve todos los documentos que tengan una matriz con ese nombre y cuyos valores de la matriz sean idénticos y estén en el mismo orden que en la consulta.

La siguiente consulta devuelve únicamente "Pen", ya que "Poster Paint" tiene un color adicional (White) y "Spray Paint" tiene los colores en otro orden.

```
db.example.find( { "Colors": ["Red","Green","Blue","Black"] } ).pretty()
```

Recuperación de documentos que coincidan con un valor de una matriz

Para buscar todos los documentos que tengan un valor determinado en una matriz, utilice la operación `find()` con el nombre de la matriz y el valor que le interese.

```
db.example.find( { "Colors": "Red" } ).pretty()
```

La operación anterior devuelve los tres documentos, ya que cada uno de ellos tiene una matriz denominada `Colors` y el valor "`Red`" en algún lugar de la matriz. Si especifica el valor "`White`", la consulta solo devolvería "Poster Paint".

Recuperación de documentos mediante operadores

La siguiente consulta devuelve todos los documentos en los que el valor de "`Inventory.OnHand`" es menor que 50.

```
db.example.find(
        { "Inventory.OnHand": { $lt: 50 } } )
```

Para obtener una lista de los operadores de consulta admitidos, consulte Operadores de consulta y proyección.

Plan de consulta

¿Cómo puedo ver **`executionStats`** para un plan de consultas?

Al determinar por qué una consulta se está ejecutando más lentamente de lo esperado, puede ser útil comprender qué `executionStats` son para el plan de consulta. `executionStats` proporciona el número de documentos devueltos desde una etapa determinada (`nReturned`), la cantidad de tiempo de ejecución empleado en cada etapa (`executionTimeMillisEstimate`) y la cantidad de tiempo que tarda en generar un plan de consulta (`planningTimeMillis`). Puede determinar las etapas más exigentes de su consulta para ayudar a enfocar sus esfuerzos de optimización a partir de la salida de `executionStats`, como se muestra en los ejemplos de consulta a continuación. El parámetro `executionStats` actualmente no admite comandos `update` ni `delete`.

> **Note**
>
> Amazon DocumentDB emula la API MongoDB 3.6 en un motor de base de datos personalizada específicamente que utiliza un sistema de almacenamiento distribuido, tolerante a fallos y de recuperación automática. Como resultado, los planes de consulta y la salida de `explain()` pueden diferir entre Amazon DocumentDB y MongoDB. Los clientes que deseen controlar su plan de consulta pueden utilizar el operador `$hint` para aplicar la selección de un índice preferido.

Ejecute la consulta que desee mejorarse en el comando `explain()` del modo siguiente.

```
db.runCommand({explain: {query document}}).
explain("executionStats").executionStats;
```

A continuación se muestra un ejemplo de operación.

```
db.fish.find({}).limit(2).explain("executionStats");
```

La salida de esta operación será similar a lo que se indica a continuación.

```
{
    "queryPlanner" : {
        "plannerVersion" : 1,
        "namespace" : "test.fish",
        "winningPlan" : {
            "stage" : "SUBSCAN",
            "inputStage" : {
                "stage" : "LIMIT_SKIP",
                "inputStage" : {
                    "stage" : "COLLSCAN"
                }
            }
        }
    },
    "executionStats" : {
        "executionSuccess" : true,
        "executionTimeMillis" : "0.063",
        "planningTimeMillis" : "0.040",
        "executionStages" : {
            "stage" : "SUBSCAN",
            "nReturned" : "2",
            "executionTimeMillisEstimate" : "0.012",
            "inputStage" : {
                "stage" : "LIMIT_SKIP",
                "nReturned" : "2",
                "executionTimeMillisEstimate" : "0.005",
                "inputStage" : {
                    "stage" : "COLLSCAN",
                    "nReturned" : "2",
                    "executionTimeMillisEstimate" : "0.005"
                }
            }
```

```
        }
    },
    "serverInfo" : {
        "host" : "enginedemo",
        "port" : 27017,
        "version" : "3.6.0"
    },
    "ok" : 1
}
```

Si está interesado en ver sólo el `executionStats` de la consulta anterior, puede utilizar el siguiente comando. En colecciones pequeñas, el procesador de consultas de Amazon DocumentDB puede optar por no utilizar un índice si las ventajas para el rendimiento son insignificantes.

```
db.fish.find({}).limit(2).explain("executionStats").executionStats;
```

Memoria caché de planes de consultas

Para optimizar el rendimiento y reducir la duración de la planificación, Amazon DocumentDB almacena internamente en caché los planes de consultas. Esto permite que las consultas con la misma forma se ejecuten directamente mediante un plan en caché.

Sin embargo, este almacenamiento en caché a veces puede provocar un retraso aleatorio para la misma consulta; por ejemplo, una consulta que normalmente tarda un segundo en ejecutarse puede tardar en ocasiones diez segundos. Esto se debe a que, con el tiempo, la instancia del lector almacenó en caché varias formas de la consulta, lo que consumió memoria. Si experimenta esta lentitud aleatoria, no es necesario que realice ninguna acción para liberar la memoria: el sistema gestionará el uso de la memoria por usted y, una vez que la memoria alcance un determinado umbral, se liberará automáticamente.

Descripción de los resultados

Si desea devolver información sobre los planes de consultas, Amazon DocumentDB admite el modo verbosidad `queryPlanner`. Los resultados `explain` devuelven el plan de consultas seleccionado elegido por el optimizador en un formato similar al siguiente:

```
{
   "queryPlanner" : {
      "plannerVersion" : <int>,
```

```
      "namespace" : <string>,
      "winningPlan" : {
         "stage" : <STAGE1>,
         ...
         "inputStage" : {
            "stage" : <STAGE2>,
            ...
            "inputStage" : {
               ...
            }
         }
      }
   }
}
```

En las siguientes secciones se definirán los resultados `explain` comunes.

Temas

- Etapa de escaneo y filtrado
- Intersección de índices
- Unión de índices
- Intersección/unión de índices múltiples
- Índice compuesto
- Etapa de clasificación
- Etapa de grupos

Etapa de escaneo y filtrado

El optimizador puede elegir uno de los siguientes escaneos:

COLLSCAN

Esta etapa es un escaneo secuencial de la colección.

```
{
    "stage" : "COLLSCAN"
}
```

IXSCAN

Esta etapa escanea las claves de índice. El optimizador puede recuperar el documento en esta etapa y esto puede provocar que se añada una etapa FETCH más adelante.

```
db.foo.find({"a": 1})
{
    "stage" : "IXSCAN",
    "direction" : "forward",
    "indexName" : <idx_name>
}
```

FETCH

Si el optimizador recuperó documentos en una etapa distinta de IXSCAN, el resultado incluirá una etapa FETCH. Por ejemplo, la consulta IXSCAN anterior puede resultar en una combinación de las etapas FETCH e IXSCAN:

```
db.foo.find({"a": 1})
{
    "stage" : "FETCH",
    "inputStage" : {
        "stage" : "IXSCAN",
        "indexName" : <idx_name>
    }
}
```

IXONLYSCAN escanea solo la clave de índice. Crear índices compuestos no evitará FETCH.

Intersección de índices

IXAND

Amazon DocumentDB puede incluir una etapa IXAND con una matriz InputStages de IXSCAN si puede utilizar la intersección de índices. Por ejemplo, podemos ver un resultado como el siguiente:

```
{
    "stage" : "FETCH",
    "inputStage" : {
        "stage" : "IXAND",
```

```
        "inputStages" : [
            {
                "stage" : "IXSCAN",
                "indexName" : "a_1"
            },
            {
                "stage" : "IXSCAN",
                "indexName" : "b_1"
            }
        ]
    }
}
```

Unión de índices

MIXOR

De forma similar a la intersección de índices, Amazon DocumentDB puede incluir una etapa `IXOR` con una matriz `inputStages` para el operador `$or`.

```
db.foo.find({"$or": [{"a": {"$gt": 2}}, {"b": {"$lt": 2}}]})
```

Para la consulta anterior, el resultado de la explicación podría tener este aspecto:

```
{
    "stage" : "FETCH",
    "inputStage" : {
        "stage" : "IXOR",
        "inputStages" : [
            {
                "stage" : "IXSCAN",
                "indexName" : "a_1"
            },
            {
                "stage" : "IXSCAN",
                "indexName" : "b_1"
            }
        ]
    }
}
```

Intersección/unión de índices múltiples

Amazon DocumentDB puede combinar varias etapas de unión o intersección de índices y, a continuación, obtener el resultado. Por ejemplo:

```
{
    "stage" : "FETCH",
    "inputStage" : {
        "stage" : "IXOR",
        "inputStages" : [
            {
                "stage" : "IXSCAN",
                ...
            },
            {
                "stage" : "IXAND",
                "inputStages" : [
                    {
                        "stage" : "IXSCAN",
                        ...
                    },
                    {
                        "stage" : "IXSCAN",
                        ...
                    }
                ]
            }
        ]
    }
}
```

El uso de las etapas de intersección o unión del índice no se ve afectado por el tipo de índice (escaso, compuesto, etc.).

Índice compuesto

El uso del índice compuesto de Amazon DocumentDB no está limitado a los subconjuntos iniciales de los campos indexados; puede utilizar el índice con la parte del sufijo, pero puede que no sea muy eficaz.

Por ejemplo, el índice compuesto de `{ a: 1, b: -1 }` puede admitir las tres consultas siguientes:

```
db.orders.find( { a: 1 } )

db.orders.find( { b: 1 } )

db.orders.find( { a: 1, b: 1 } )
```

Etapa de clasificación

Si hay un índice en las claves de clasificación solicitadas, Amazon DocumentDB puede usar el índice para obtener la clasificación. En ese caso, el resultado no incluirá una etapa `SORT`, sino más bien una etapa `IXSCAN`. Si el optimizador prefiere una ordenación simple, incluirá una etapa como esta:

```
{
    "stage" : "SORT",
    "sortPattern" : {
        "a" : 1,
        "b" : -1
    }
}
```

Etapa de grupos

Amazon DocumentDB admite dos estrategias de grupo diferentes:

- `SORT_AGGREGATE`: agregado de clasificación en disco.
- `HASH_AGGREGATE`: agregado de hash en memoria.

Planificador de consultas v2

El nuevo planificador de consultas para Amazon DocumentDB (versión 2.0 del planificador) incluye características avanzadas de optimización de consultas y un rendimiento mejorado. La versión 2.0 del planificador para Amazon DocumentDB 5.0 mejora el rendimiento hasta 10 veces con respecto a la versión anterior cuando se utilizan los operadores `find` y `update` con índices. Las mejoras en el rendimiento se deben principalmente al uso de planes de indexación más óptimos y a que se habilita el escaneo de índices para operadores como los operadores de negación (`$neq`, `$nin`) y anidados `$elementMatch`. Las consultas de la versión 2.0 del planificador se ejecutan más rápido gracias a mejores técnicas de estimación de costos, algoritmos optimizados y una estabilidad mejorada. La versión 2.0 de Planner también es compatible con el filtro APIs de caché del plan, lo que mejora

la estabilidad del planificador. Con esta característica, Amazon DocumentDB 5.0 ahora ofrece la posibilidad de seleccionar entre las distintas versiones del planificador de consultas.

Temas

- Requisitos previos
- Selección de la versión 2.0 del planificador como planificador de consultas predeterminado
- Prácticas recomendadas
- Limitaciones
- Mejoras en operadores Find y Update
- API del filtro de caché del plan
- Posibles diferencias de comportamiento entre el planificador, versión 1.0, 2.0 y MongoDB
- La versión 2.0 del planificador cierra la brecha de comportamiento con MongoDB

Requisitos previos

Para usar la versión 2.0 del planificador, se deben cumplir los siguientes requisitos previos:

- La versión 2.0 del planificador está disponible en todas las regiones en las que está disponible la versión 5.0 del motor.
- Para optar por utilizar la versión 2.0 como planificador de consultas predeterminado, el clúster debe tener el parche del motor 3.0.15902 o posterior de la versión 5.0 de Amazon DocumentDB. Para obtener información sobre los pasos para actualizar el parche a la última versión del motor, consulte Actualización de un parche a la versión del motor de un clúster.
- Para configurar la versión 2.0 del planificador como el planificador de consultas predeterminado, necesita permisos de IAM para actualizar los grupos de parámetros del clúster.

Selección de la versión 2.0 del planificador como planificador de consultas predeterminado

Siga los siguientes pasos para seleccionar 2.0 como el planificador de consultas predeterminado desde la consola o la CLI:

- Siga los pasos en Modificación de parámetros de clúster de Amazon DocumentDB para modificar el grupo de parámetros del clúster.

- Para el parámetro denominado «plannerVersion», cambie el valor a 2.0 para indicar la versión 2.0 del planificador.
- Seleccione Aplicar inmediatamente (si selecciona Aplicar al reiniciar, la selección no será válida hasta el siguiente reinicio del clúster).

Prácticas recomendadas

Para obtener los resultados esperados, utilice las siguientes prácticas recomendadas cuando aplique la versión 2.0 del planificador:

- En un clúster global, seleccione el mismo valor de la `plannerVersion` (1.0 o 2.0) en los grupos de parámetros del clúster para ambas regiones. Tenga en cuenta que seleccionar diferentes versiones del planificador en las regiones principales y secundarias puede provocar que el comportamiento y el rendimiento de las consultas no sea constante.
- La actualización a la versión 2.0 del planificador durante un período de mantenimiento programado o durante períodos de tráfico reducido será lo menos molesto, ya que puede haber un aumento en las tasas de error si se cambia la versión del planificador cuando las cargas de trabajo se están ejecutando activamente.
- La versión 2.0 del planificador funciona de manera óptima con el shell de MongoDB, versión 5.0.

Limitaciones

Las siguientes limitaciones se aplican a la versión 2.0 del planificador:

- La versión 2.0 del planificador no es compatible con los clústeres elásticos, que recurrirán a la versión 1.0 del planificador.
- La versión 2.0 del planificador no admite la agregación ni los comandos distintos, por lo que se recurrirá a la versión 1.0 del planificador.
- El filtro de caché del plan de la versión 2.0 del planificador no admite consultas que contengan expresiones regulares, búsquedas de texto, geoespaciales, jsonschema ni `$expr` en filtros.

Mejoras en operadores **`Find`** y **`Update`**

La versión 2.0 del planificador optimiza las operaciones fundamentales, incluidos los comandos `find`, `update`, `delete` y `find-and-modify`. Las siguientes secciones con pestañas muestran las

capacidades mejoradas de los índices, así como las mejoras en el rendimiento de las consultas con la versión 2.0 del planificador:

Enhanced index support

- La versión 2.0 del planificador añade compatibilidad con índices para los operadores de negación, incluidos `$nin`, `$ne`, `$not {eq}`, `$not {in}`, `$type` y `$elemMatch`.

```
Sample Document: { "x": 10, "y": [1, 2, 3] }

db.foo.createIndex({ "x": 1, "y": 1 })
db.foo.find({ "x": {$nin: [20, 30] }})
db.foo.find({"x":{ $type: "string" }})

db.foo.createIndex({"x.y": 1})
db.foo.find({"x":{$elemMatch:{"y":{$elemMatch:{"$gt": 3 }}}}})
```

- La versión 2.0 del planificador utiliza índices dispersos o parciales incluso cuando `$exists` no está presente en la expresión de consulta.

```
Sample Document: {"name": "Bob", "email": "example@fake.com" }

Using Planner Version 1.0, you can specify the command as shown below:
db.foo.find({email: "example@fake.com", email: {$exists: true}})

Using Planner Version 2.0, you can specify command without $exists:
db.foo.find({ email: "example@fake.com" })
```

- La versión 2.0 del planificador utilizará índices parciales incluso cuando la condición de consulta no coincida exactamente con la expresión del filtro de índice parcial.

```
Sample Document: {"name": "Bob", "age": 34}
db.foo.createIndex({"age":1},{partialFilterExpression:{"age":{$lt:50}}})

With Planner Version 1.0, index is used only when the query condition meets the
 partial
 index filter criterion:
     db.foo.find({"age":{$lt:50}})

With Planner Version 2.0, index is used even when the query condition doesn't meet
 the index
criterion:
```

```
db.foo.find({"age":{$lt:30}})
```

- La versión 2.0 del planificador utiliza un escaneo parcial del índice con consultas de $elemMatch.

```
Sample Document: {"name": "Bob", "age": [34,35,36]}
db.foo.createIndex({"age":1},{partialFilterExpression:{"age":{$lt:50,$gt:20}}})
db.foo.find({age:{$elemMatch:{$lt:50,$gt:20}}})
```

- La versión 2.0 del planificador incluye soporte con escaneo de índices para `$regex`, sin necesidad de incluir `$hint` en el código de la aplicación. `$regex` solo admite búsquedas de indexación por prefijo.

```
Sample Document: { "x": [1, 2, 3], "y": "apple" }
db.foo.createIndex({ "x": 1, "y": 1 })
db.foo.find({"y":{ $regex: "^a" }})
```

- La versión 2.0 del planificador mejora el rendimiento de las consultas que utilizan índices de claves múltiples, con condiciones de igualdad en los campos de claves múltiples.

```
Sample Document: {"x": [1, 2, 3],
"y": 5}
db.foo.createIndex({"x": 1, "y":1})
db.foo.find({"x": 2,
"y": {$gt: 1}}).limit(1)
```

- La versión 2.0 del planificador mejora el rendimiento de las consultas que utilizan filtros múltiples, especialmente en colecciones con documentos de más de 8 KB.

```
Sample Document: {"x": 2,
"y": 4,
"z": 9,
"t": 99}
db.foo.find({$and: [{"x": {$gt : 1}, "y": {$gt : 3}, "z": {$lt : 10},
"t":{$lt : 100}}]})
```

- La versión 2.0 del planificador mejora el rendimiento de las consultas cuando se utiliza el operador `$in` con un índice compuesto al eliminar la etapa de clasificación.

```
Sample Document: {"x": 2,
"y": 4,
"z": 9,
```

```
"t": 99}
db.foo.createIndex({"x":1, "y":1})
db.foo.find({"x":2,
"y":$in:[1,2,3,4]}).sort({x:1,y:1})
```

También mejora el rendimiento de las consultas que utilizan índices de varias claves con `$in` elementos.

```
Sample Document: {"x": [1, 2, 3]}
db.foo.createIndex({"x": 1})
db.foo.find("x":{$in:[>100 elements]})
```

Query performance improvements

- La versión 2.0 del planificador mejora el rendimiento de las consultas que utilizan filtros múltiples, especialmente en colecciones con documentos de más de 8 KB.

```
Sample Document: {"x": 2,
"y": 4,
"z": 9,
"t": 99}
db.foo.find({$and: [{"x": {$gt : 1}, "y": {$gt : 3}, "z": {$lt : 10},
"t":{$lt : 100}}]})
```

- La versión 2.0 del planificador mejora el rendimiento de las consultas cuando se utiliza el operador `$in` con un índice compuesto al eliminar la etapa de clasificación.

```
Sample Document: {"x": 2,
"y": 4,
"z": 9,
"t": 99}
db.foo.createIndex({"x":1, "y":1})
db.foo.find({"x":2,
"y":$in:[1,2,3,4]}).sort({x:1,y:1})
```

También mejora el rendimiento de las consultas que utilizan índices de claves múltiples con elementos `$in`.

```
Sample Document: {"x": [1, 2, 3]}
db.foo.createIndex({"x": 1})
```

```
db.foo.find("x":{$in:[>100 elements]})
```

API del filtro de caché del plan

> **Note**
>
> El índice de texto no es compatible con el filtro de caché del plan.

- La versión 2.0 del planificador añade compatibilidad con la característica de filtro de índices que permite especificar una lista de índices que puede utilizar una forma de consulta específica. Se puede acceder a esta característica a través de la API y se puede controlar desde el servidor. Si experimenta una regresión de consultas, esta característica le ofrece una opción más rápida y flexible para mitigar el problema sin tener que modificar el código de la aplicación.

  ```
  db.runCommand({ planCacheSetFilter: <collection>, query: <query>,
  sort: <sort>, // optional,
  indexes: [ <index1>, <index2>, ...],
  comment: <any> // optional})
  ```

  Para mostrar todos los filtros de la colección, use el siguiente comando:

  ```
  db.runCommand(
  {
  planCacheListFilters: <collection>
  }
  )
  ```

  Este comando muestra todos los filtros de índice de la colección. Ejemplo de código de salida:

  ```
  {
  "filters" : [
  {
  "query" : {a: "@", b: "@"},
  "sort" : {a: 1},
  "indexes" : [
  <index1>,
  ...
  ]
  ```

```
},
...
],
"ok": 1
}
```

- Puede utilizar dos campos nuevos del resultado del comando `explain` para analizar el filtrado de índices de la versión 2.0 del planificador: `indexFilterSet` y `indexFilterApplied`. `indexFilterSet` se establece en «verdadero» si hay un filtro de índice establecido en la colección que coincide con la forma de la consulta. `indexFilterApplied` se establece en «verdadero» si, y solo si, la consulta aplicó un filtro de índice y eligió un plan mediante el uso de un índice de la lista de filtros.

  Puede borrar el filtro de índice con el siguiente comando:

```
db.runCommand(
{
planCacheClearFilters: <collection>>
query: <query pattern>, // optional
sort: <sort specification>, // optional
comment: <any>. //optional
}
)
```

  Para borrar todos los filtros de la colección «foo», use el siguiente comando:

```
db.runCommand({planCacheClearFilters: "foo"})
```

  Para borrar una forma de consulta específica con cualquier tipo, puede copiar y pegar la forma de consulta desde el resultado de `planCacheListFilters`:

```

db.runCommand({planCacheClearFilters: "foo", query: {a: @}})
```

  Para borrar una forma de consulta específica con un campo especificado en cualquier tipo, puede copiar y pegar la forma de consulta desde el resultado de `planCacheListFilters`:

```
db.runCommand({planCacheClearFilters: "foo", query: {a: @},sort: {a: 1}})
```

Posibles diferencias de comportamiento entre el planificador, versión 1.0, 2.0 y MongoDB

En algunos casos extremos, es posible que la versión 2.0 del planificador produzca resultados que varíen ligeramente de los resultados de MongoDB. En esta sección se describen algunos ejemplos de estas posibilidades.

$(update) and $(projection)

- En algunos casos, los operadores `$(update)` y `$(projection)` de MongoDB pueden comportarse de forma diferente a la versión 1.0 del planificador de Amazon DocumentDB. A continuación se muestran algunos ejemplos:

```
db.students_list.insertMany( [ { _id: 5, student_ids: [ 100, 200 ], grades: [ 95,
 100 ], grad_year: [ 2024, 2023 ] } ] )
```

```
db.students_list.updateOne({ student_ids: 100, grades: 100, grad_year: 2024 },
{ $set: { “grad_year.$”: 2025 } }
```

  - Planificador, versión 1.0: actualiza el campo 2022.
  - MongoDB: actualiza el campo 2022.
  - Planificador, versión 2.0: actualiza el campo 2021.

- ```
  db.col.insert({x:[1,2,3]})
  db.col.update({$and:[{x:1},{x:3}]},{$set:{"x.$":500}})
  ```

  - Planificador, versión 1.0: actualiza aleatoriamente el primer elemento coincidente.
  - MongoDB: actualiza aleatoriamente el primer elemento coincidente.
  - Planificador, versión 2.0: no realiza actualizaciones.

- ```
  db.col.insert({x:[1,2,3]})
  db.col.find()
  ```

  - Planificador, versión 1.0: selecciona aleatoriamente el elemento coincidente.
  - MongoDB: selecciona aleatoriamente el elemento coincidente.
  - Planificador, versión 2.0: no realiza ninguna selección.

- ```
  db.col.insert({x:100})
  ```
  ```

```
db.col.update({x:100},{x:100})
```

  - Planificador, versión 1.0: cambios en el recuento nModified.
  - MongoDB: cambios en el recuento nModified.
  - Planificador, versión 2.0: el recuento nModified no cambia cuando se actualiza con el mismo valor.
- Cuando se usa el operador `$(update)` con `$setOnInsert`, la versión 1.0 del planificador y MongoDB arrojan un error, pero la versión 2.0 del planificador no.
- Si se cambia el nombre de un campo que no existe a `$field`, se produce un error en la versión 2.0 del planificador, mientras que no se producen actualizaciones en la versión 1.0 del planificador ni en MongoDB.

Index behavior

- La versión 2.0 del planificador arroja un error cuando se aplica `$hint` con un índice inadecuado, mientras que la versión 1.0 del planificador y MongoDB no lo hacen.

```
// Insert
db.col.insert({x:1})
db.col.insert({x:2})
db.col.insert({x:3})

// Create index on x with partialFilter Expression {x:{$gt:2}}
db.col.createIndex({x:1},{partialFilterExpression:{x:{$gt:2}}})

// Mongodb allows hint on the following queries
db.col.find({x:1}).hint("x_1")
// result is no documents returned because {x:1} is not indexed by the partial
 index
// Without $hint mongo should return {x:1}, thus the difference in result between
 COLSCAN and IXSCAN

DocumentDB will error out when $hint is applied on such cases.
db.col.find({x:1}).hint("x_1")
Error: error: {
    "ok" : 0,
    "operationTime" : Timestamp(1746473021, 1),
    "code" : 2,
    "errmsg" : "Cannot use Hint for this Query. Index is multi key index , partial
 index or sparse index and query is not optimized to use this index."
```

```
}

rs0:PRIMARY> db.runCommand({"planCacheSetFilter": "col", "query": { location:
 {$nearSphere: {$geometry: {type: "Point", coordinates: [1, 1]}}}}, "indexes":
 ["name_1"]})
{
    "ok" : 0,
    "operationTime" : Timestamp(1750815778, 1),
    "code" : 303,
    "errmsg" : "Unsupported query shape for index filter $nearSphere"
}
```

- `$near` no puede utilizar `$hint({“$natural”:1})` en la versión 2.0 del planificador.

```
// indexes present are index on x and geo index

rs0:PRIMARY> db.usarestaurants.getIndexes()
[
    {
        "v" : 4,
        "key" : {
            "_id" : 1
        },
        "name" : "_id_",
        "ns" : "test.usarestaurants"
    },
    {
        "v" : 4,
        "key" : {
            "location" : "2dsphere"
        },
        "name" : "location_2dsphere",
        "ns" : "test.usarestaurants",
        "2dsphereIndexVersion" : 1
    }
]

// Planner Version 2.0 will throw an error when $hint is applied with index "x_1"
rs0:PRIMARY> db.usarestaurants.find({    "location":{       "$nearSphere":{
         "$geometry":{             "type":"Point",             "coordinates":
[                -122.3516,                47.6156             ]          },
          "$minDistance":1,          "$maxDistance":2000       }    } }, {
  "name":1 }).hint({"$natural": 1})
Error: error: {
```

```
    "ok" : 0,
    "operationTime" : Timestamp(1746475524, 1),
    "code" : 291,
    "errmsg" : "unable to find index for $geoNear query"
}

// Planner Version 1.0 and MongoDB will not throw an error
 db.usarestaurants.find({    "location":{       "$nearSphere":{
  "$geometry":{             "type":"Point",             "coordinates":[
            -122.3516,                47.6156             ]          },
        "$minDistance":1,          "$maxDistance":2000       }    } }, {
  "name":1 }).hint({"$natural": 1})
{ "_id" : ObjectId("681918e087dadfd99b7f0172"), "name" : "Noodle House" }
```

- Si bien MongoDB admite escaneos completos de índices de expresiones regulares, la versión 2.0 del planificador admite el escaneo de índices de expresiones regulares solo en los campos con prefijo.

```
// index on x
db.col.createIndex({x:1})

// index scan is used only for prefix regexes
rs0:PRIMARY> db.col.find({x: /^x/}).explain()
{
    "queryPlanner" : {
        "plannerVersion" : 2,
        "namespace" : "test.col",
        "winningPlan" : {
            "stage" : "IXSCAN",
            "indexName" : "x_1",
            "direction" : "forward",
            "indexCond" : {
                "$and" : [
                    {
                        "x" : {
                            "$regex" : /^x/
                        }
                    }
                ]
            },
            "filter" : {
                "x" : {
                    "$regex" : /^x/
```

```
                }
            }
        }
    },
    "indexFilterSet" : false,
    "indexFilterApplied" : false,
    "ok" : 1,
    "operationTime" : Timestamp(1746474527, 1)
}

// COLSCAN is used for non-prefix regexes
rs0:PRIMARY> db.col.find({x: /x$/}).explain()
{
    "queryPlanner" : {
        "plannerVersion" : 2,
        "namespace" : "test.col",
        "winningPlan" : {
            "stage" : "COLLSCAN",
            "filter" : {
                "x" : {
                    "$regex" : /x$/
                }
            }
        }
    },
    "indexFilterSet" : false,
    "indexFilterApplied" : false,
    "ok" : 1,
    "operationTime" : Timestamp(1746474575, 1)
```

- Existen algunas diferencias inherentes al uso de filtros de caché del plan con la versión 2.0 del planificador en comparación con MongoDB. Si bien la versión 2.0 del planificador no admite especificar la «proyección» y la «intercalación» con los filtros de caché del plan, MongoDB sí lo hace. Sin embargo, el filtro de índice de MongoDB solo está en memoria y se pierde tras el reinicio. La versión 2.0 del planificador conserva los filtros de índice mediante reinicios y parches.

Others

- El formato de los registros de auditoría de DML cuando se utiliza la versión 2.0 del planificador varía ligeramente de la versión 1.0.

```
command -  db.col.find({x:1})

************** Audit logs generated ******************

// v1 format for dml audit logs
{"atype":"authCheck","ts":1746473479983,"timestamp_utc":"2025-05-05
 19:31:19.983","remote_ip":"127.0.0.1:47022","users":
[{"user":"serviceadmin","db":"test"}],"param":
{"command":"find","ns":"test.col","args":{"batchSize":101,"filter":
{"x":1},"find":"col","limit":18446744073709551615,"lsid":
{"id":{"$binary":"P6RCGz9ZS4iWBSSHWXW15A==","$type":"4"},"uid":
{"$binary":"6Jo8PisnEi3dte03+pJFjdCyn/5cGQL8V2KqaoWsnk8=","$type":"0"}},"maxScan":18446744

// v2 formal for dml audit logs
{"atype":"authCheck","ts":1746473583711,"timestamp_utc":"2025-05-05
 19:33:03.711","remote_ip":"127.0.0.1:37754","users":
[{"user":"serviceadmin","db":"test"}],"param":
{"command":"find","ns":"test.col","args":{"find":"col","filter":{"x":1},"lsid":
{"id":{"$binary":"nJ88TGCSSd
+BeD2+ZtrhQg==","$type":"4"}},"$db":"test"},"result":0}}
```

- La condición del índice como parte del plan explicativo:

```
rs0:PRIMARY> db.col.createIndex({index1:1})
{
 "createdCollectionAutomatically" : false,
 "numIndexesBefore" : 1,
 "numIndexesAfter" : 2,
 "ok" : 1,
 "operationTime" : Timestamp(1761149251, 1)
}
```

La versión 2.0 del planificador explica el resultado del plan, mostrando la condición del índice y el filtro:

```
rs0:PRIMARY> db.col.find({$and:[{price:{$eq:300}},{item:
{$eq:"apples"}}]}).explain()
{
 "queryPlanner" : {
  "plannerVersion" : 2,
  "namespace" : "test.col",
```

```
  "winningPlan" : {
   "stage" : "IXSCAN",
   "indexName" : "price_1",
   "direction" : "forward",
   "indexCond" : {
    "$and" : [
     {
      "price" : {
       "$eq" : 300
      }
     }
    ]
   },
   "filter" : {
    "$and" : [
     {
      "item" : {
       "$eq" : "apples"
      }
     }
    ]
   }
  }
 },
 "indexFilterSet" : false,
 "indexFilterApplied" : false,
 "ok" : 1,
 "operationTime" : Timestamp(1761149497, 1)
}
```

Resultado del plan explicativo de la versión 1.0 del planificador:

```
rs0:PRIMARY> db.col.find({$and:[{price:{$eq:300}},{item:
{$eq:"apples"}}]}).explain()
{
 "queryPlanner" : {
  "plannerVersion" : 1,
  "namespace" : "test.col",
  "winningPlan" : {
   "stage" : "IXSCAN",
   "indexName" : "price_1",
   "direction" : "forward"
  }
```

```
 },
 "ok" : 1,
 "operationTime" : Timestamp(1761149533, 1)
}
```

La versión 2.0 del planificador cierra la brecha de comportamiento con MongoDB

Hay algunas áreas en las que la versión 2.0 del planificador cierra las brechas de comportamiento con MongoDB:

- La versión 2.0 del planificador permite la búsqueda de índices numéricos en matrices aplanadas para `$elemMatch`:

```
doc: {"x" : [ [ { "y" : 1 } ] ] }

// Planner Version 2 and mongo
> db.bar.find({"x.0": {$elemMatch: {y: 1}}})
{ "_id" : ObjectId("68192947945e5846634c455a"), "x" : [ [ { "y" : 1 } ] ] }
> db.bar.find({"x": {$elemMatch: {"0.y": 1}}})
{ "_id" : ObjectId("68192947945e5846634c455a"), "x" : [ [ { "y" : 1 } ] ] }

//Whereas Planner Version 1 wouldn't return any results.
> db.bar.find({"x.0": {$elemMatch: {y: 1}}})
> db.bar.find({"x": {$elemMatch: {"0.y": 1}}})
```

- Si bien la versión 1.0 del planificador excluía las cadenas en la proyección, el comportamiento de la versión 2.0 del planificador se alinea con MongoDB y las trata como valores literales.

```
// Planner V2/ MongoDB
> db.col.find()
{ "_id" : ObjectId("681537738aa101903ed2fe05"), "x" : 1, "y" : 1 }
> db.col.find({},{x:"string"})
{ "_id" : ObjectId("681537738aa101903ed2fe05"), "x" : "string" }

// Planner V1 treats strings as exclude in projection
rs0:PRIMARY> db.col.find()
{ "_id" : ObjectId("68153744d42969f11d5cca72"), "x" : 1, "y" : 1 }
rs0:PRIMARY> db.col.find({},{x:"string"})
{ "_id" : ObjectId("68153744d42969f11d5cca72"), "y" : 1 }
```

- La versión 2.0 del planificador, como MongoDB, no permite la proyección en los mismos campos «x» y «x.a»:

```
// Planner version 2/MongoDB will error out
> db.col.find()
{ "_id" : ObjectId("68153da2012265816bc9ba23"), "x" : [ { "a" : 1 }, 3 ] }
 db.col.find({},{"x.a":1,"x":1}) // error

// Planner Version 1 does not error out
db.col.find()
{ "_id" : ObjectId("68153da2012265816bc9ba23"), "x" : [ { "a" : 1 }, 3 ] }

db.col.find({},{"x.a":1,"x":1})
{ "_id" : ObjectId("68153d60143af947c720d099"), "x" : [ { "a" : 1 }, 3 ] }
```

- La versión 2.0 del planificador, como MongoDB, permite la proyección en subdocumentos:

```
// Planner Version2/MongoDB supports projections on subdocuments
 db.col.find()
{ "_id" : ObjectId("681542d8f35ace71f0a50004"), "x" : [ { "y" : 100 } ] }
> db.col.find({},{"x":{"y":1}})
{ "_id" : ObjectId("681542b7a22d548e4ac9ddea"), "x" : [ { "y" : 100 } ] }

// Planner V1 throws error if projection is subdocument
 db.col.find()
{ "_id" : ObjectId("681542d8f35ace71f0a50004"), "x" : [ { "y" : 100 } ] }
rs0:PRIMARY> db.col.find({},{"x":{"y":1}})
Error: error: {
    "ok" : 0,
    "operationTime" : Timestamp(1746223914, 1),
    "code" : 2,
    "errmsg" : "Unknown projection operator y"
}
```

- Con la versión 2.0 del planificador, como MongoDB, la proyección no admite campos después del operador $:

```
// Mongo and Planner Version 2 will error out
  db.col.find()
{ "_id" : ObjectId("68155fa812f843439b593f3f"), "x" : [ { "a" : 100 } ] }
 db.col.find({"x.a":100},{"x.$.a":1}) - // error

// v1 will not error out
```

```
 db.col.find()
{ "_id" : ObjectId("68155fa812f843439b593f3f"), "x" : [ { "a" : 100 } ] }
db.col.find({"x.a":100},{"x.$.a":1})
{ "_id" : ObjectId("68155dee13b051d58239cd0a"), "x" : [ { "a" : 100 } ] }
```

- La versión 2.0 del planificador, como MongoDB, permite el uso de `$hint`:

```
// v1 will error out on $hint if there are no filters
db.col.find({}).hint("x_1")
Error: error: {
    "ok" : 0,
    "operationTime" : Timestamp(1746466616, 1),
    "code" : 2,
    "errmsg" : "Cannot use Hint for this Query. Index is multi key index , partial
 index or sparse index and query is not optimized to use this index."
}


// Mongo and Planner Version 2 will allow $hint usage
 db.col.find({}).hint("x_1")
{ "_id" : ObjectId("6818f790d5ba9359d68169cf"), "x" : 1 }
```

Planificador de consultas v3

La versión 3 de Planner de Amazon DocumentDB 8.0 admite 21 etapas de agregación, incluidas 6 etapas nuevas. Planner V3 incluye soporte integrado para distintos comandos. Ofrece una mejora del rendimiento general de hasta el doble en comparación con Planner v2 en Amazon DocumentDB 5.0. Todas las funciones y operadores nuevos de Amazon DocumentDB 8.0 son compatibles con Planner v3. Entre las nuevas etapas de agregación de Amazon DocumentDB 8.0 compatibles con Planner v3 se incluyen $replaceWith, $VectorSearch, $merge, $set, $unset y $bucket. Planner v3 también admite nuevas funciones y operadores en Amazon DocumentDB 8.0, como Collation, Views, $merge, $pow, $rand, $DateTrunc, $, $. dateToParts dateFromParts

Temas

- Requisitos previos
- Seleccionar la versión 3.0 del planificador como planificador de consultas predeterminado
- Prácticas recomendadas
- Limitaciones

- Mejoras en operadores aggregate y distinct
- Posibles diferencias de comportamiento entre las versiones 1.0, 3.0 y MongoDB del planificador

Requisitos previos

Los siguientes requisitos previos se aplican a la versión 3.0 del planificador:

- La versión 3.0 de Planner está disponible en todas las regiones en las que está disponible la versión 8.0 del motor.
- La versión 3.0 de Planner es el planificador de consultas predeterminado cuando se selecciona la versión 8.0 del motor.

Seleccionar la versión 3.0 del planificador como planificador de consultas predeterminado

Si ha cambiado el planificador de consultas predeterminado en Amazon DocumentDB 8.0 y necesita volver al planificador v3, puede hacerlo desde la consola o desde la CLI:

- Siga los pasos en Modificación de parámetros de clúster de Amazon DocumentDB para modificar el grupo de parámetros del clúster.
- Para el parámetro denominado 'PlannerVersion', cambie el valor a 3.0 para indicar la versión 3.0 del planificador.
- Seleccione Aplicar inmediatamente (si selecciona Aplicar al reiniciar, la selección no será válida hasta el siguiente reinicio del clúster).

Prácticas recomendadas

Para obtener los resultados esperados, utilice las siguientes prácticas recomendadas al aplicar la versión 3.0 del planificador:

- En un clúster global, seleccione el mismo `plannerVersion` valor (1.0, 2.0 o 3.0) en los grupos de parámetros del clúster para ambas regiones. Tenga en cuenta que seleccionar diferentes versiones del planificador en las regiones principales y secundarias puede provocar que el comportamiento y el rendimiento de las consultas no sea constante.
- La actualización a la versión 3.0 del planificador durante un período de mantenimiento programado o durante períodos de tráfico reducido será lo menos molesto, ya que las tasas de error pueden

aumentar si se cambia la versión del planificador cuando las cargas de trabajo se están ejecutando activamente.

Limitaciones

Las siguientes limitaciones se aplican a la versión 3.0 del planificador:

- La versión 3.0 de Planner no es compatible con los clústeres elásticos, que recurrirán a la versión 1.0 de Planner.

- Si bien Planner v1 permite el uso de «PlanHint» para garantizar que el optimizador de consultas seleccione un plan de consultas específico, Planner v3 no permite el uso de «PlanHint» y se basa en optimizaciones internas para elegir el mejor plan para la consulta en cuestión.

Mejoras en operadores **`aggregate`** y **`distinct`**

La versión 3.0 de Planner introduce mejoras en las etapas de $aggregate y en el comando $distinct. Las siguientes son algunas de las mejoras más destacables.

- Cuando es posible, el planificador sitúa las etapas de $match en una fase más temprana del proceso, lo que reduce el número de documentos procesados en las etapas posteriores.

```
//Planner v1
db.orders.aggregate([
  { $project: { customerId: 1, orderDate: 1, totalAmount: 1 } },
  { $match: { customerId: { $gt: 1000 } } }
])

// Planner v3 pulls up the match since customerId exists in original documents
// Optimized internally as:
db.orders.aggregate([
  { $match: { customerId: { $gt: 1000 } } },  // Pulled up before project
  { $project: { customerId: 1, orderDate: 1, totalAmount: 1 } }
])
```

- El planificador combina automáticamente las etapas $lookup y $unwind cuando funcionan en el mismo campo, lo que reduce el procesamiento intermedio de datos y mejora el rendimiento.

```
                 Example query:
//Planner v1
db.orders.aggregate([
  { $lookup: { from: "products", localField: "productId", foreignField: "_id", as:
 "productInfo" } },
  { $unwind: "$productInfo" },
  { $project: { orderDate: 1, "productInfo.name": 1, "productInfo.price": 1 } }
])

// Planner version 3.0 optimizes this internally by coalescing the $lookup and
 $unwind stages
```

- La versión 3.0 de Planner presenta una nueva estrategia de ejecución de Distinct Scan que mejora significativamente el rendimiento de distintas operaciones con índices de cardinalidad bajos.

```
                 Example query:
//// If there is a low cardinality index on "category", you may see a query plan like
 below
db.explain().products.distinct("category")

"queryPlanner" : {
        "plannerVersion" : 3,
        "namespace" : "db.products",
        "winningPlan" : {
                "stage" : "AGGREGATE",
                "inputStage" : {
                        "stage" : "DISTINCT_SCAN",
                        "inputStage" : {
                                "stage" : "IXONLYSCAN",
                                "indexName" : "category_1",
                                "direction" : "forward"
                        }
                }
        }
}
```

Posibles diferencias de comportamiento entre las versiones 1.0, 3.0 y MongoDB del planificador

En algunos casos extremos, es posible que la versión 3.0 del planificador produzca resultados ligeramente diferentes a los de la versión 1.0 del planificador. En esta sección se describen algunos ejemplos de estas posibilidades.

Feature Differences

- En una colección vacía o cuando etapas anteriores, como una coincidencia, filtran todos los documentos, Planner v1 muestra el «campo» de salida :0. Planner v3 y MongoDB no darán ningún resultado.
- Con Plannerv1, {"$skip» :n} no omite si la etapa anterior devolvió menos de n documentos. Plannerv3 y MongoDB omiten correctamente independientemente del número de documentos devueltos.
- Cuando no existe una colección externa a la que se hace referencia en $lookup, plannerv1 arroja un error. Planner v3 y MongoDB tratan la colección externa como una colección vacía y ejecutan $lookup.

```
db.coll.aggregate([
    {$lookup: {from: "does_not_exist", localField: "a", foreignField: "a", as:
 "c"}}
])
```

- Solo Planner v1 permitirá usar múltiples $search en una canalización. Planner v2/v3 arrojará un error y MongoDB no lo admite.

```
VectorSearch = { "$search": { "vectorSearch": {
   "vector": [0.2, 0.5, 0.8],
   "path": "vectorEmbedding",
   "similarity": "cosine",
   "k": 2,
   "efSearch": 1
   }}}
db.coll.aggregate([VectorSearch, VectorSearch])
```

- Solo Planner v3 funciona cuando la etapa VectorSearch no es la primera etapa. En este caso, MongoDB generará un error y Planner v1 no admite la etapa $VectorSearch.

```
VectorSearch = { {"$vectorSearch": {
    "queryVector": [0.2, 0.5, 0.8],
    "path": "vectorEmbedding",
    "similarity": "euclidean",
    "limit": 4,
    "numCandidates": 100} }

db.coll.aggregate([$match:{}, VectorSearch])
```

Consulta de datos geoespaciales con Amazon DocumentDB

En esta sección se explica cómo puede consultar datos geoespaciales con Amazon DocumentDB. Tras leer esta sección, podrá responder a cómo almacenar, consultar e indexar datos geoespaciales en Amazon DocumentDB.

Temas

- Descripción general de
- Indexación y almacenamiento de datos geoespaciales
- Consulta de datos geoespaciales
- Limitaciones

Descripción general de

Los casos de uso más comunes de la tecnología geoespacial incluyen el análisis de proximidad de sus datos. Por ejemplo, “buscar todos los aeropuertos en un radio de 50 millas de Seattle” o “encontrar los restaurantes más cercanos desde una ubicación determinada”. Amazon DocumentDB utiliza la especificación GeoJSON para representar datos geoespaciales. GeoJSON es una especificación de código abierto para el formato JSON de formas en un espacio de coordenadas. Las coordenadas GeoJSON capturan tanto la longitud como la latitud y representan las posiciones en una esfera similar a la Tierra.

Indexación y almacenamiento de datos geoespaciales

Amazon DocumentDB utiliza el tipo GeoJSON de tipo “Punto” para almacenar datos geoespaciales. Cada documento (o subdocumento) de GeoJSON se compone generalmente de dos campos:

- tipo: la forma que se representa, que indica a Amazon DocumentDB cómo interpretar el campo “coordenadas”. En este momento, Amazon DocumentDB solo admite puntos
- coordenadas: un par de latitud y longitud representado como un objeto en una matriz: [longitud, latitud]

Amazon DocumentDB también utiliza índices de 2dsphere para indexar datos geoespaciales. Amazon DocumentDB admite puntos de indexación. Amazon DocumentDB admite consultas de proximidad con la indexación de 2dsphere.

Consideremos un escenario en el que está creando una aplicación para un servicio de entrega de alimentos. Desea almacenar el par de latitudes y longitudes de varios restaurantes en Amazon DocumentDB. Para ello, primero le recomendamos que cree un índice en el campo geoespacial que contenga el par de latitud y longitud.

```
use restaurantsdb
db.usarestaurants.createIndex({location:"2dsphere"})
```

La salida de este comando tendrá un aspecto similar al siguiente:

```
{
 "createdCollectionAutomatically" : true,
 "numIndexesBefore" : 1,
 "numIndexesAfter" : 2,
 "ok" : 1
}
```

Una vez que haya creado un índice, puede empezar a insertar datos en su colección de Amazon DocumentDB.

```
db.usarestaurants.insert({
   "state":"Washington",
   "city":"Seattle",
   "name":"Thai Palace",
   "rating": 4.8,
   "location":{
      "type":"Point",
      "coordinates":[
         -122.3264,
         47.6009
```

```
      ]
   }
});

db.usarestaurants.insert({
   "state":"Washington",
   "city":"Seattle",
   "name":"Noodle House",
   "rating": 4.8,
   "location":{
      "type":"Point",
      "coordinates":[
        -122.3517,
         47.6159
      ]
   }
});

db.usarestaurants.insert({
   "state":"Washington",
   "city":"Seattle",
   "name":"Curry House",
   "rating": 4.8,
   "location":{
      "type":"Point",
      "coordinates":[
         -121.4517,
         47.6229
      ]
   }
});
```

Consulta de datos geoespaciales

Amazon DocumentDB admite consultas de proximidad, inclusión e intersección de datos geoespaciales. Un buen ejemplo de consulta de proximidad es buscar todos los puntos (todos los aeropuertos) que están a menos de una distancia determinada y a más de una distancia de otro punto (ciudad). Un buen ejemplo de consulta de inclusión es buscar todos los puntos (todos los aeropuertos) que se encuentran en un area/polygon (estado de Nueva York) específico. Un buen ejemplo de consulta de intersección es buscar un polígono (estado) que se interseque con un punto (ciudad). Puede utilizar los siguientes operadores geoespaciales para obtener información a partir de sus datos.

- **`$nearSphere`**- `$nearSphere` es un operador de búsqueda que permite buscar puntos del más cercano al más lejano de un punto GeoJSON.
- **`$geoNear`**- `$geoNear` es un operador de agregación que permite calcular la distancia en metros desde un punto GeoJSON.
- **`$minDistance`**- `$minDistance` es un operador de búsqueda que se utiliza junto con `$nearSphere` o `$geoNear` para filtrar documentos que se encuentran al menos a la distancia mínima especificada desde el punto central.
- **`$maxDistance`**- `$maxDistance` es un operador de búsqueda que se utiliza junto con `$nearSphere` o `$geoNear` para filtrar documentos que se encuentran como máximo a la distancia máxima especificada desde el punto central.
- **`$geoWithin`**- `$geoWithin` es un operador de búsqueda que permite buscar documentos con datos geoespaciales que existan completamente dentro de una forma específica, como un polígono.
- **`$geoIntersects`**- `$geoIntersects` es un operador de búsqueda que permite buscar documentos cuyos datos geoespaciales se crucen con un objeto GeoJSON específico.

> **Note**
>
> `$geoNeary` `$nearSphere` requieren un índice de 2dsphere en el campo GeoJSON que utilice en la consulta de proximidad.

Ejemplo 1

En este ejemplo, aprenderá a buscar todos los restaurantes (puntos) ordenados por la distancia más cercana a una dirección (punto).

Para realizar una consulta de este tipo, puede `$geoNear` utilizar el cálculo de la distancia entre un conjunto de puntos y otro punto. También puede agregar el `distanceMultiplier` para medir la distancia en kilómetros.

```
db.usarestaurants.aggregate([
   {
      "$geoNear":{
         "near":{
            "type":"Point",
```

```
            "coordinates":[
               -122.3516,
               47.6156
            ]
         },
         "spherical":true,
         "distanceField":"DistanceKilometers",
         "distanceMultiplier":0.001
      }
   }
])
```

El comando anterior devolvería los restaurantes ordenados por distancia (del más cercano al más lejano) desde el punto especificado. La salida de este comando tendrá un aspecto similar al siguiente.

```
{ "_id" : ObjectId("611f3da985009a81ad38e74b"), "state" : "Washington", "city" :
 "Seattle", "name" : "Noodle House", "rating" : 4.8, "location" : { "type" : "Point",
 "coordinates" : [ -122.3517, 47.6159 ] }, "DistanceKilometers" : 0.03422834547294996 }
{ "_id" : ObjectId("611f3da185009a81ad38e74a"), "state" : "Washington", "city" :
 "Seattle", "name" : "Thai Palace", "rating" : 4.8, "location" : { "type" : "Point",
 "coordinates" : [ -122.3264, 47.6009 ] }, "DistanceKilometers" : 2.5009390081704277 }
{ "_id" : ObjectId("611f3dae85009a81ad38e74c"), "state" : "Washington", "city" :
 "Seattle", "name" : "Curry House", "rating" : 4.8, "location" : { "type" : "Point",
 "coordinates" : [ -121.4517, 47.6229 ] }, "DistanceKilometers" : 67.52845344856914 }
```

Para limitar el número de resultados de una consulta, utilice la opción `limit` o `num`.

`limit`:

```
db.usarestaurants.aggregate([
   {
      "$geoNear":{
         "near":{
            "type":"Point",
            "coordinates":[
               -122.3516,
               47.6156
            ]
         },
         "spherical":true,
         "distanceField":"DistanceKilometers",
```

```
         "distanceMultiplier":0.001,
         "limit": 10
      }
   }
])
```

num:

```
db.usarestaurants.aggregate([
   {
      "$geoNear":{
         "near":{
            "type":"Point",
            "coordinates":[
               -122.3516,
               47.6156
            ]
         },
         "spherical":true,
         "distanceField":"DistanceKilometers",
         "distanceMultiplier":0.001,
         "num": 10
      }
   }
])
```

> **Note**
>
> La etapa `$geoNear` admite las opciones `limit` y `num` para especificar el número máximo de documentos que se van a devolver. `$geoNear` devuelve un máximo de 100 documentos de forma predeterminada si no se especifican las opciones `limit` o `num`. Esto se anula con el valor de la etapa `$limit`, si está presente, y el valor es inferior a 100.

Ejemplo 2

En este ejemplo, aprenderá a buscar todos los restaurantes (puntos) en un radio de 2 kilómetros de una dirección (punto) específica. Para realizar una consulta de este tipo, puede utilizar `$nearSphere` con un `$minDistance` mínimo y un `$maxDistance` máximo desde un punto GeoJSON

```
db.usarestaurants.find({
   "location":{
      "$nearSphere":{
         "$geometry":{
            "type":"Point",
            "coordinates":[
               -122.3516,
               47.6156
            ]
         },
         "$minDistance":1,
         "$maxDistance":2000
      }
   }
},
{
   "name":1
})
```

El comando anterior devolvería los restaurantes a una distancia máxima de 2 kilómetros del punto especificado. La salida de este comando tendrá un aspecto similar al siguiente.

```
{ "_id" : ObjectId("611f3da985009a81ad38e74b"), "name" : "Noodle House" }
```

Limitaciones

Amazon DocumentDB no admite consultas ni indexación de polígonos,, LineString y. MultiPoint MultiPolygon MultiLineString GeometryCollection

Índice parcial

Un índice parcial indexa los documentos de una colección que cumplen un criterio de filtro especificado. La característica de índice parcial se admite en los clústeres basados en instancias de Amazon DocumentDB 5.0.

Temas

- Creación de un índice parcial
- Operadores admitidos
- Consulta mediante un índice parcial

- Funcionalidades de indexación parcial
- Limitaciones del índice parcial

Creación de un índice parcial

Para crear un índice parcial, utilice el método `createIndex()` con la opción `partialFilterExpression`. Por ejemplo, la siguiente operación crea un índice compuesto único en la colección de pedidos que indexa los documentos que tienen un `OrderID` y cuyo campo `isDelivered` es true:

```
db.orders.createIndex(
  {"category": 1, "CustomerId": 1, "OrderId": 1},
  {"unique": true, "partialFilterExpression":
    {"$and": [
      {"OrderId": {"$exists": true}},
      {"isDelivered": {"$eq": false}}
    ]}
  }
)
```

Operadores admitidos

- $eq
- $exists
- $and (solo en el nivel superior)
- $gt/$gte/$lt/$lte (el escaneo de índices solo se usa cuando el filtro, basado en la consulta, coincide exactamente con la expresión del filtro parcial) (consulte las limitaciones)

Consulta mediante un índice parcial

Los siguientes patrones de consulta son posibles con índices parciales:

- El predicado de la consulta coincide exactamente con la expresión del filtro de índice parcial:

```
db.orders.find({"$and": [
    {"OrderId": {"$exists": true}},
```

```
    {"isDelivered": {"$eq": false}}
  ]}).explain()
```

- El resultado esperado del filtro de consulta es un subconjunto lógico del filtro parcial:

```
db.orders.find({"$and": [
    {"OrderId": {"$exists": true}},
    {"isDelivered": {"$eq": false}},
    {"OrderAmount": {"$eq": "5"}}
  ]}).explain()
```

- Se puede utilizar un subpredicado de la consulta junto con otros índices:

```
db.orders.createIndex({"anotherIndex":1})
db.orders.find({ "$or": [
      {"$and": [
        {"OrderId": {"$exists": true}},
        {"isDelivered": {"$eq": false}}
      ]},
      {"anotherIndex": {"$eq": 5}}
    ]
  }).explain()
```

> **Note**
>
> Un planificador de consultas puede optar por utilizar un escaneo de colecciones en lugar de un escaneo de índices si es eficiente hacerlo. Esto suele ocurrir en el caso de colecciones o consultas muy pequeñas que devuelven una gran parte de una colección.

Funcionalidades de indexación parcial

Lista de índices parciales

Enumere los índices parciales con partialFilterExpression mediante la operación `getIndex`. Por ejemplo, la operación `getIndex` emitida en las listas de índices parciales con los campos clave, nombre y partialfilterExpressions:

```
db.orders.getIndexes()
```

En este ejemplo, se devuelve la siguiente salida:

```
[
  {
    "v" : 4,
    "key" : {
      "_id" : 1
    },
    "name" : "_id_",
    "ns" : "ecommerceApp.orders"
  },
  {
    "v" : 4,
    "unique" : true,
    "key" : {
      "category" : 1,
      "" : 1,
      "CustomerId" : 1,
      "OrderId" : 1
    },
    "name" : "category_1_CustID_1_OrderId_1",
    "ns" : "ecommerceApp.orders",
    "partialFilterExpression" : {
      "$and" : [
        {"OrderId": {"$exists": true}},
        {"isDelivered": {"$eq": false}}
      ]
    }
  }
]
```

Expresión de filtro parcial múltiple en la misma clave:orden

Se pueden crear diferentes índices parciales para las mismas combinaciones de campos (clave:orden). Estos índices deben tener un nombre distinto.

```
db.orders.createIndex(
  {"OrderId":1},
  {
    name:"firstPartialIndex",
    partialFilterExpression:{"OrderId":{"$exists": true}}
  }
)
```

```
db.orders.createIndex(
  {"OrderId":1},
  {
    name:"secondPartialIndex",
    partialFilterExpression:{"OrderId":{"$gt": 1000}}
  }
)
```

Ejecute la operación `getIndexes` para enumerar todos los índices de la colección:

```
db.orders.getIndexes()
```

En estos ejemplos, se devuelve la siguiente salida:

```
[
  {
    "v" : 4,
    "key" : {
      "_id" : 1
    },
    "name" : "_id_",
    "ns" : "ecommerceApp.orders"
  },
  {
    "v" : 4,
    "key" : {
      "OrderId" : 1
    },
    "name" : "firstPartialIndex",
    "ns" : "ecommerceApp.orders",
    "partialFilterExpression" : {"OrderId":{"$exists": true}}
  },
  {
    "v" : 4,
    "key" : {
      "OrderId" : 1
    },
    "name" : "secondPartialIndex",
    "ns" : "ecommerceApp.orders",
    "partialFilterExpression" : {"OrderId":{"$gt": 1000}}
  }
]
```

> **Important**
>
> Los nombres de los índices deben ser diferentes y se deben eliminar solo por su nombre.

Índices con propiedades parciales y TTL

También puede crear índices con propiedades parciales y TTL mediante la especificación de las opciones `partialFilterExpression` y `expireAfterSeconds` durante la creación del índice. Esto le permite tener más control sobre qué documentos se eliminan ahora de una colección.

Por ejemplo, puede tener un índice TTL que identifique los documentos que se van a eliminar después de un periodo de tiempo determinado. Ahora puede establecer condiciones adicionales sobre cuándo eliminar documentos mediante la opción de índice parcial:

```
db.orders.createIndex(
    { "OrderTimestamp": 1 },
    {
        expireAfterSeconds: 3600 ,
        partialFilterExpression: { "isDelivered": { $eq: true } }
    }
)
```

En este ejemplo, se devuelve la siguiente salida:

```
{
        "createdCollectionAutomatically" : false,
        "numIndexesBefore" : 1,
        "numIndexesAfter" : 2,
        "ok" : 1,
        "operationTime" : Timestamp(1234567890, 1)
}
```

Ejecute la operación `getIndexes` para enumerar los índices de la colección:

```
db.orders.getIndexes()
[
    {
        "v" : 4,
        "key" : {
```

```
            "_id" : 1
        },
        "name" : "_id_",
        "ns" : "test.orders"
    }
```

En este ejemplo, se devuelve la siguiente salida:

```
[
    {
        "v": 4,
        "key": {
            "_id": 1
        },
        "name": "_id_",
        "ns": "ecommerceApp.orders"
    },
    {
        "v": 4,
        "key": {
            "OrderTimestamp": 1
        },
        "name": "OrderTimestamp_1",
        "ns": "ecommerceApp.orders",
        "partialFilterExpression": {
            "isDelivered": {
                "$eq": true
            }
        },
        "expireAfterSeconds": 3600
    }
]
```

Limitaciones del índice parcial

La característica de índice parcial tiene las siguientes limitaciones:

- Las consultas de desigualdad en Amazon DocumentDB solo utilizarán un índice parcial cuando el predicado del filtro de consultas coincida exactamente con el `partialFilterExpression` y sea del mismo tipo de datos.

> **Note**
>
> Ni siquiera `$hint` se puede usar para forzar el IXSCAN en el caso anterior.

En el siguiente ejemplo, `partialFilterExpression` solo se aplica a `field1`, pero no a `field2`:

```
db.orders.createIndex(
  {"OrderAmount": 1},
  {"partialFilterExpression": { OrderAmount : {"$gt" : 5}}}
)

db.orders.find({OrderAmount : {"$gt" : 5}}) // Will use partial index
db.orders.find({OrderAmount : {"$gt" : 6}}) // Will not use partial index
db.orders.find({OrderAmount : {"$gt" : Decimal128(5.00)}}) // Will not use partial
 index
```

- No se admite `partialFilterExpression` con los operadores de matriz. La siguiente operación generará un error:

```
db.orders.createIndex(
  {"CustomerId":1},
  {'partialFilterExpression': {'OrderId': {'$eq': [1000, 1001, 1002]}}}
)
```

- Los siguientes operadores no se admiten en el campo partialFilterExpression:
  - `$all` (operador de matrices)
  - `$mod` (operador de matrices)
  - `$or`
  - `$xor`
  - `$not`
  - `$nor`
- El tipo de datos de la expresión de filtro y el filtro deben ser iguales.

Búsquedas de texto con Amazon DocumentDB

La función de búsqueda de texto completo nativa de Amazon DocumentDB (Text Index v1) le permite realizar búsquedas de texto en conjuntos de datos textuales de gran tamaño mediante índices de texto especiales. En esta sección se describen las funcionalidades de la característica de índice de texto y se proporcionan los pasos para crear y utilizar índices de texto en Amazon DocumentDB. También se enumeran las limitaciones de la búsqueda de texto.

Temas

- Funcionalidades admitidas
- Uso del índice de texto de Amazon DocumentDB
- Diferencias con MongoDB
- Prácticas recomendadas y directrices
- Índice de texto V2
- Limitaciones

Funcionalidades admitidas

La búsqueda de texto de Amazon DocumentDB admite las siguientes funcionalidades compatibles con la API de MongoDB:

- Cree índices de texto en un solo campo.
- Cree índices de texto compuestos que incluyan más de un campo de texto.
- Haga búsquedas de una o varias palabras.
- Controle los resultados de la búsqueda mediante ponderaciones.
- Ordene los resultados de la búsqueda por puntuación.
- Usa el índice de texto en la canalización de agregación.
- Busque la frase exacta.

Uso del índice de texto de Amazon DocumentDB

Para crear un índice de texto en un campo que contenga datos de cadena, especifique la cadena “texto” como se muestra a continuación:

Índice de campo único:

```
db.test.createIndex({"comments": "text"})
```

Este índice admite consultas de búsqueda de texto en el campo de cadena de “comentarios” de la colección especificada.

Cree un índice de texto compuesto en más de un campo de cadena:

```
db.test.createIndex({"comments": "text", "title":"text"})
```

Este índice admite consultas de búsqueda de texto en los campos de cadena de “comentarios” y “título” de la colección especificada. Puede especificar hasta 30 campos al crear un índice de texto compuesto. Una vez creadas, las consultas de búsqueda de texto consultarán todos los campos indexados.

> **Note**
>
> Solo se permite un índice de texto en cada colección.

Visualización de un índice de texto en una colección de Amazon DocumentDB

Puede utilizar `getIndexes()` en su colección para identificar y describir índices, incluidos los índices de texto, como se muestra en el siguiente ejemplo:

```
rs0:PRIMARY> db.test.getIndexes()
[
   {
      "v" : 4,
      "key" : {
         "_id" : 1
      },
      "name" : "_id_",
      "ns" : "test.test"
   },
   {
      "v" : 1,
      "key" : {
         "_fts" : "text",
```

```
         "_ftsx" : 1
      },
      "name" : "contents_text",
      "ns" : "test.test",
      "default_language" : "english",
      "weights" : {
         "comments" : 1
      },
      "textIndexVersion" : 1
   }
]
```

Una vez que haya creado un índice, empiece a insertar datos en su colección de Amazon DocumentDB.

```
db.test.insertMany([{"_id": 1, "star_rating": 4, "comments": "apple is red"},
                    {"_id": 2, "star_rating": 5, "comments": "pie is delicious"},
                    {"_id": 3, "star_rating": 3, "comments": "apples, oranges - healthy
 fruit"},
                    {"_id": 4, "star_rating": 2, "comments": "bake the apple pie in the
 oven"},
                    {"_id": 5, "star_rating": 5, "comments": "interesting couch"},
                    {"_id": 6, "star_rating": 5, "comments": "interested in couch for
 sale, year 2022"}])
```

Ejecución de consultas de búsqueda de texto

Ejecute una consulta de búsqueda de texto de una sola palabra

Necesitará utilizar los operadores `$text` y `$search` para hacer búsquedas de texto. El ejemplo siguiente devuelve todos los documentos en los que el campo indexado de texto contiene la cadena “manzana” o “manzana” en otros formatos, como “manzanas”:

```
db.test.find({$text: {$search: "apple"}})
```

Salida:

La salida de este comando tendrá un aspecto similar al siguiente:

```
{ "_id" : 1, "star_rating" : 4, "comments" : "apple is red" }
{ "_id" : 3, "star_rating" : 3, "comments" : "apples, oranges - healthy fruit" }
```

```
{ "_id" : 4, "star_rating" : 2, "comments" : "bake the apple pie in the oven" }
```

Ejecución de una búsqueda de texto de varias palabras

También puede hacer búsquedas de texto de varias palabras en sus datos de Amazon DocumentDB. El siguiente comando devuelve documentos con un campo de texto indexado que contiene las palabras “manzana” o “tarta”:

```
db.test.find({$text: {$search: "apple pie"}})
```

Salida:

La salida de este comando tendrá un aspecto similar al siguiente:

```
{ "_id" : 1, "star_rating" : 4, "comments" : "apple is red" }
{ "_id" : 2, "star_rating" : 5, "comments" : "pie is delicious" }
{ "_id" : 3, "star_rating" : 3, "comments" : "apples, oranges - healthy fruit" }
{ "_id" : 4, "star_rating" : 2, "comments" : "bake the apple pie in the oven" }
```

Ejecución de una búsqueda de texto con frases de varias palabras

Para una búsqueda de frases de varias palabras, utilice este ejemplo:

```
db.test.find({$text: {$search: "\"apple pie\""}})
```

Salida:

El comando anterior devuelve documentos con un campo de texto indexado que contiene la frase exacta “tarta de manzana”. La salida de este comando tendrá un aspecto similar al siguiente:

```
{ "_id" : 4, "star_rating" : 2, "comments" : "bake the apple pie in the oven" }
```

Ejecución de una búsqueda de texto con filtros

También puede combinar la búsqueda de texto con otros operadores de consulta para filtrar los resultados en función de criterios adicionales:

```
db.test.find({$and: [{star_rating: 5}, {$text: {$search: "interest"}}]})
```

Salida:

El comando anterior devuelve los documentos con un campo de texto indexado que contiene cualquier forma de “interés” y una “calificación_por_estrellas” igual a 5. La salida de este comando tendrá un aspecto similar al siguiente:

```
{ "_id" : 5, "star_rating" : 5, "comments" : "interesting couch" }
{ "_id" : 6, "star_rating" : 5, "comments" : "interested in couch for sale, year
 2022" }
```

Limitación del número de documentos devueltos en una búsqueda de texto

Puede optar por restringir el número de documentos devueltos mediante `limit`:

```
db.test.find({$and: [{star_rating: 5}, {$text: {$search: "couch"}}]}).limit(1)
```

Salida:

El comando anterior devuelve un resultado que cumple con el filtro:

```
{ "_id" : 5, "star_rating" : 5, "comments" : "interesting couch" }
```

Ordenación de los resultados por puntuación de texto

En el siguiente ejemplo, se ordenan los resultados de la búsqueda de texto por puntuación de texto:

```
db.test.find({$text: {$search: "apple"}}, {score: {$meta: "textScore"}}).sort({score:
 {$meta: "textScore"}})
```

Salida:

El comando anterior devuelve los documentos con un campo de texto indexado que contiene la palabra “manzana” o “manzana” en otros formatos, como “manzanas”, y ordena el resultado en función de la relación del documento con el término de búsqueda. La salida de este comando tendrá un aspecto similar al siguiente:

```
{ "_id" : 1, "star_rating" : 4, "comments" : "apple is red", "score" :
 0.6079270860936958 }
{ "_id" : 3, "star_rating" : 3, "comments" : "apples, oranges - healthy fruit",
 "score" : 0.6079270860936958 }
```

```
{ "_id" : 4, "star_rating" : 2, "comments" : "bake the apple pie in the oven",
 "score" : 0.6079270860936958 }
```

`$text` y `$search` también son compatibles con los comandos `aggregate`, `count`, `findAndModify`, `update` y `delete`.

Operadores de agregación

Canalización de agregación mediante **`$match`**

```
db.test.aggregate(
   [{ $match: { $text: { $search: "apple pie" } } }]
)
```

Salida:

El comando anterior devuelve los siguientes resultados:

```
{ "_id" : 1, "star_rating" : 4, "comments" : "apple is red" }
{ "_id" : 3, "star_rating" : 3, "comments" : "apple - a healthy fruit" }
{ "_id" : 4, "star_rating" : 2, "comments" : "bake the apple pie in the oven" }
{ "_id" : 2, "star_rating" : 5, "comments" : "pie is delicious" }
```

Una combinación de otros operadores de agregación

```
db.test.aggregate(
   [
      { $match: { $text: { $search: "apple pie" } } },
      { $sort: { score: { $meta: "textScore" } } },
      { $project: { score: { $meta: "textScore" } } }
   ]
)
```

Salida:

El comando anterior devuelve los siguientes resultados:

```
{ "_id" : 4, "score" : 0.6079270860936958 }
{ "_id" : 1, "score" : 0.3039635430468479 }
{ "_id" : 2, "score" : 0.3039635430468479 }
```

```
{ "_id" : 3, "score" : 0.3039635430468479 }
```

Especifique varios campos al crear un índice de texto

Puede asignar ponderaciones a un máximo de tres campos del índice de texto compuesto. La ponderación predeterminada asignada a un campo en un índice de texto es uno (1). La ponderación es un parámetro opcional y debe estar en el rango de 1 a 100 000.

```
db.test.createIndex(
   {
     "firstname": "text",
     "lastname": "text",
     ...
   },
   {
     weights: {
       "firstname": 5,
       "lastname":10,
       ...
     },
     name: "name_text_index"
   }
 )
```

Diferencias con MongoDB

La característica de índice de texto de Amazon DocumentDB utiliza un índice invertido con un algoritmo de frecuencia de términos. Los índices de texto son dispersos de forma predeterminada. Debido a las diferencias en la lógica de análisis, los delimitadores de tokenización y otros, es posible que no se devuelva el mismo conjunto de resultados que MongoDB para el mismo conjunto de datos o forma de consulta.

Existen las siguientes diferencias adicionales entre el índice de texto de Amazon DocumentDB y MongoDB:

- No se admiten los índices compuestos que utilizan índices que no sean de texto.
- Los índices de texto de Amazon DocumentDB no distinguen entre mayúsculas y minúsculas.
- Solo se admite el idioma inglés con el índice de texto.
- No se admite la indexación de texto de campos matriciales (o de varias claves). Por ejemplo, no se podrá crear un índice de texto en “a” con el documento {“a”: [“manzana”, “tarta”]}.

- No se admite la indexación de texto con caracteres comodín.
- No se admiten índices de texto únicos.
- No se admite la exclusión de un término.

Prácticas recomendadas y directrices

- Para obtener un rendimiento óptimo en las consultas de búsqueda de texto que implican ordenar por puntuaciones de texto, se recomienda crear el índice de texto antes de cargar los datos.
- Los índices de texto requieren almacenamiento adicional para poder disponer de una copia interna optimizada de los datos indexados. Esto tiene implicaciones de costos adicionales.

Índice de texto V2

Amazon DocumentDB 8.0 presenta una nueva versión del índice de texto (V2) que cambia el analizador de búsqueda de texto subyacente para ofrecer una mayor compatibilidad con MongoDB.

Además de las funcionalidades que ofrecen los índices de texto de la versión 1, los índices de texto de la versión 2 también ofrecen la siguiente compatibilidad:

- Cuando es posible, el planificador mueve las etapas de $match al principio del proceso, lo que reduce la cantidad de documentos procesados en las etapas posteriores.

```
rs0:PRIMARY> db.coll.createIndex({ "a": "text" });
rs0:PRIMARY> db.coll.find()
{ "_id" : 1, "a" : "jane.doe_1234@company.com" }
{ "_id" : 2, "a" : "janedoe@company.com" }
{ "_id" : 3, "a" : "/home/user/company/thesis.pdf" }
{ "_id" : 4, "a" : "/home/user/path/jane.pdf" }
{ "_id" : 5, "a" : "http://www.company.com/path" }
{ "_id" : 6, "a" : "https://company.com/path/../home" }

//Sample queries
rs0:PRIMARY> db.coll.find({ $text: { $search: "jane" } });
rs0:PRIMARY> db.coll.find({ $text: { $search: "doe_1234" } });
rs0:PRIMARY> db.coll.find({ $text: { $search: "http" } });

// Text Index V1 results
None
```

```
// Text Index V2 results
{ "_id" : 1, "a" : "jane.doe_1234@company.com" }
{ "_id" : 4, "a" : "/home/user/path/jane.pdf" }
{ "_id" : 5, "a" : "http://www.company.com/path" }
```

Limitaciones

La búsqueda de texto tiene las siguientes limitaciones en Amazon DocumentDB:

- Los índices de texto almacenan los lexemas y su información de posición. El tamaño combinado de todos los lexemas y su información de posición, en un solo documento, está limitado a 1 MB.

Solución de problemas de Amazon DocumentDB

En las siguientes secciones, se proporciona información acerca de cómo solucionar los problemas que puedan surgir al utilizar Amazon DocumentDB (con compatibilidad con MongoDB).

Temas

- Solución de problemas de conexión
- Índices de solución de problemas
- Solución de problemas de rendimiento y utilización de recursos
- Recopilación de elementos no utilizados en Amazon DocumentDB

Solución de problemas de conexión

¿Tiene problemas para conectarse? A continuación se muestran algunos escenarios comunes y cómo resolverlos.

Temas

- No se puede conectar a un punto de conexión de Amazon DocumentDB
- Comprobación de una conexión a una instancia de Amazon DocumentDB
- Conexión a un punto de conexión no válido
- La configuración del controlador afecta al número de conexiones

No se puede conectar a un punto de conexión de Amazon DocumentDB

Al intentar conectarse a Amazon DocumentDB, el siguiente es uno de los mensajes de error más comunes que podría encontrarse.

```
connecting to: mongodb://docdb-2018-11-08-21-47-27.cluster-ccuszbx3pn5e.us-east-
1.docdb.amazonaws.com:27017/
2018-11-14T14:33:46.451-0800 W NETWORK [thread1] Failed to connect to
172.31.91.193:27017 after 5000ms milliseconds, giving up.
2018-11-14T14:33:46.452-0800 E QUERY [thread1] Error: couldn't connect to server
docdb-2018-11-08-21-47-27.cluster-ccuszbx3pn5e.us-east-1.docdb.amazonaws.com:27017,
connection attempt failed :
connect@src/mongo/shell/mongo.js:237:13
```

```
@(connect):1:6
exception: connect failed
```

Este mensaje de error normalmente significa que el cliente (el shell de mongo, en este ejemplo) no puede obtener acceso al punto de conexión de Amazon DocumentDB. Esto puede deberse a varios motivos:

Temas

- Conexión desde puntos de conexión públicos
- Conexiones entre regiones
- Conexión desde diferentes Amazon VPC
- Conexiones entrantes en bloques del grupo de seguridad
- Problema de preferencia de lectura del controlador Java Mongo

Conexión desde puntos de conexión públicos

Está intentando conectarse a un clúster de Amazon DocumentDB directamente desde un portátil o un equipo de desarrollo local.

Se producirá un error al intentar conectarse a un clúster de Amazon DocumentDB directamente desde un dispositivo de punto de conexión público, como una laptop o una máquina de desarrollo local. Amazon DocumentDB solo está diseñado para una nube privada virtual (VPC) y actualmente no admite puntos de conexión públicos. Por lo tanto, no puede conectarse directamente a su clúster de Amazon DocumentDB desde un portátil o un entorno de desarrollo local que esté fuera de la VPC.

Para conectarse a un clúster de Amazon DocumentDB desde fuera de una VPC de Amazon, puede utilizar un túnel de SSH. Para obtener más información, consulte Conexión a un clúster de Amazon DocumentDB desde fuera de una Amazon VPC. Asimismo, si su entorno de desarrollo se encuentra en una VPC distinta, también puede utilizar una interconexión de VPC y conectarse a su clúster de Amazon DocumentDB desde otra VPC de Amazon que esté en la misma región o en una región diferente.

Conexiones entre regiones

Está intentando conectarse a un clúster de Amazon DocumentDB de otra región.

Si intenta conectarse a un clúster de Amazon DocumentDB desde una instancia de Amazon EC2 en una región distinta a la región del clúster (por ejemplo, si intenta conectarse a un clúster en región

este de EE. UU. (Norte de Virginia) (us-east-1) desde la región oeste de EE. UU. (Oregón) (us-west-2), la conexión fallará.

Para verificar la región del clúster de Amazon DocumentDB, ejecute el siguiente comando. La región está en el punto de conexión.

```
aws docdb describe-db-clusters \
   --db-cluster-identifier sample-cluster \
   --query 'DBClusters[*].Endpoint'
```

La salida de esta operación será similar a lo que se indica a continuación.

```
[
    "sample-cluster.node.us-east-1.docdb.amazonaws.com"
]
```

Para verificar la región de la instancia EC2, ejecute el siguiente comando.

```
 aws ec2 describe-instances \
     --query 'Reservations[*].Instances[*].Placement.AvailabilityZone'
```

La salida de esta operación será similar a lo que se indica a continuación.

```
[
    [
        "us-east-1a"
    ]
]
```

Conexión desde diferentes Amazon VPC

Está intentando conectarse a un clúster de Amazon DocumentDB desde una VPC distinta de la VPC de Amazon en la que se ha implementado el clúster.

Si tanto el clúster de Amazon DocumentDB como la instancia Amazon EC2 se encuentran en la misma Región de AWS, pero no en la misma Amazon VPC, no puede conectarse directamente al clúster de Amazon DocumentDB a menos que esté habilitada la interconexión de VPC entre las dos VPC de Amazon.

Para comprobar la Amazon VPC de su instancia de Amazon DocumentDB, ejecute el siguiente comando.

```
aws docdb describe-db-instances \
   --db-instance-identifier sample-instance \
   --query 'DBInstances[*].DBSubnetGroup.VpcId'
```

Para comprobar la Amazon VPC de su instancia de Amazon EC2, ejecute el siguiente comando.

```
aws ec2 describe-instances \
   --query 'Reservations[*].Instances[*].VpcId'
```

Conexiones entrantes en bloques del grupo de seguridad

Está intentando conectarse a un clúster de Amazon DocumentDB, pero el grupo de seguridad del clúster no admite conexiones entrantes en el puerto del clúster (el puerto predeterminado es el 27017).

Supongamos que el clúster de Amazon DocumentDB y la instancia Amazon EC2 se encuentran en la misma región y la VPC de Amazon, y utiliza el mismo grupo de seguridad de Amazon VPC. Si no puede conectarse al clúster de Amazon DocumentDB, es probable que la causa sea que el grupo de seguridad (es decir, el firewall) del clúster no permite las conexiones entrantes en el puerto que eligió para el clúster de Amazon DocumentDB (el puerto predeterminado es el 27017).

Para verificar el puerto del clúster de Amazon DocumentDB, ejecute el siguiente comando.

```
aws docdb describe-db-clusters \
   --db-cluster-identifier sample-cluster \
   --query 'DBClusters[*].[DBClusterIdentifier,Port]'
```

Para obtener el grupo de seguridad de Amazon DocumentDB de su clúster, ejecute el siguiente comando.

```
aws docdb describe-db-clusters \
   --db-cluster-identifier sample-cluster \
   --query 'DBClusters[*].[VpcSecurityGroups[*],VpcSecurityGroupId]'
```

Para comprobar las reglas de entrada del grupo de seguridad, consulte los temas siguientes de la documentación de Amazon EC2:

- Autorización del tráfico de entrada para sus instancias de Linux

- Autorización del tráfico de entrada para sus instancias de Windows

Problema de preferencia de lectura del controlador Java Mongo

No se respetan las preferencias de lectura del cliente y algunos clientes no pueden escribir en Amazon DocumentDB después de una conmutación por error a menos que reinicien.

Este problema, descubierto por primera vez en Java Mongo Driver 3.7.x, se produce cuando un cliente establece una conexión con Amazon DocumentDB mediante `MongoClientSettings` y, específicamente, al encadenar el método `applyToClusterSettings`. La configuración del clúster de MongoClient se puede definir mediante varios métodos diferentes, `hosts()` como `requiredReplicaSetName()` y `mode()`.

Cuando el cliente especifica solo un host en el método `hosts()`, el modo se establece en `ClusterConnectionMode.SINGLE` lugar de `ClusterConnectionMode.MULTIPLE`. Esto hace que el cliente ignore la preferencia de lectura y solo se conecte al servidor configurado en `hosts()`. Por lo tanto, incluso si la configuración del cliente se inicializa como se muestra a continuación, todas las lecturas seguirán yendo a la principal en lugar de a la secundaria.

```
final ServerAddress serverAddress0 = new ServerAddress("cluster-endpoint", 27317));
    final MongoCredential credential = MongoCredential.createCredential("xxx",
            "admin", "xxxx".toCharArray());
    final MongoClientSettings settings = MongoClientSettings.builder()
            .credential(credential)
            .readPreference(ReadPreference.secondaryPreferred())
            .retryWrites(false)
            .applyToSslSettings(builder -> builder
                    .enabled(false))
            .applyToClusterSettings(builder -> builder.hosts(
                            Arrays.asList(serverAddress0
                            ))
                    .requiredReplicaSetName("rs0"))
            .build();
    MongoClient mongoClient = MongoClients.create(settings);
```

Caso de conmutación por error

Con la configuración de conexión del cliente anterior, si se produce una conmutación por error y se retrasa la actualización del registro de DNS en el punto de conexión del escritor del clúster, el cliente seguirá intentando realizar escrituras en el antiguo escritor (que ahora se lee tras la conmutación por

error). Esto provoca un error en el servidor (no en el principal) que el controlador de Java no gestiona adecuadamente (el problema aún se está investigando). Por lo tanto, el cliente puede quedar en mal estado hasta que se reinicie el servidor de aplicaciones, por ejemplo.

Existen dos soluciones alternativas para ello:

- Los clientes que se conecten a Amazon DocumentDB mediante una cadena de conexión no tendrán este problema, ya que `ClusterConnectionMode` se establecerá en `MULTIPLE` al configurar la preferencia de lectura.

  ```
  MongoClientURI mongoClientURI = new MongoClientURI("mongodb://usr:pass:cluster-
  endpoint:27317/test?ssl=false&replicaSet=rs0&readpreference=secondaryPreferred");
  MongoClient mongoClient = MongoClients.create(mongoClientURI.getURI());
  ```

  O usar el constructor `MongoClientSettings` con el método `applyConnectionString`.

  ```
  final MongoClientSettings settings = MongoClientSettings.builder()
          .credential(credential)
          .applyConnectionString(new ConnectionString("usr:pass:cluster-endpoint:27317/
  test?ssl=false&replicaSet=rs0&readpreference=secondaryPreferred"))
          .retryWrites(false)
          .applyToSslSettings(builder # builder
                  .enabled(false))
          .build();
  MongoClient mongoClient = MongoClients.create(settings);
  ```

- Establecido `ClusterConnectionMode` explícitamente en `MULTIPLE`. Esto solo es necesario cuando se usa `applyToClusterSettings` y `hosts().size() == 1`.

  ```
  final ServerAddress serverAddress0 = new ServerAddress("cluster-endpoint", 27317));
  final MongoCredential credential = MongoCredential.createCredential("xxx","admin",
   "xxxx".toCharArray());
  final MongoClientSettings settings = MongoClientSettings.builder()
      .credential(credential)
      .readPreference(ReadPreference.secondaryPreferred())
      .retryWrites(false)
      .applyToSslSettings(builder # builder
      .enabled(false))
      .applyToClusterSettings(builder # builder
                  .hosts(Arrays.asList(serverAddress0))
                  .requiredReplicaSetName("rs0"))
                  .mode(ClusterConnectionMode.MULTIPLE))
  ```

```
    .build();
MongoClient mongoClient = MongoClients.create(settings);
```

Comprobación de una conexión a una instancia de Amazon DocumentDB

Puede comprobar la conexión a un clúster mediante las herramientas habituales de Windows o de Linux.

En un terminal de Linux o Unix, puede comprobar la conexión escribiendo lo siguiente (sustituya `cluster-endpoint` por el punto de conexión y `port` por el puerto de la instancia):

```
nc -zv cluster-endpoint port
```

A continuación se muestra un ejemplo de una operación y el valor devuelto:

```
nc -zv docdbTest.d4c7nm7stsfc0.us-west-2.docdb.amazonaws.com 27017

Connection to docdbTest.d4c7nm7stsfc0.us-west-2.docdb.amazonaws.com 27017 port [tcp/*]
 succeeded!
```

Conexión a un punto de conexión no válido

Si se conecta a un clúster de Amazon DocumentDB y utiliza un punto de conexión del clúster que no es válido, aparece un error similar al siguiente.

```
mongo --ssl \
   --host sample-cluster.node.us-east-1.docdb.amazonaws.com:27017 \
   --sslCAFile global-bundle.pem \
   --username <user-name> \
   --password <password>
```

El resultado tendrá este aspecto:

```
MongoDB shell version v3.6
connecting to: mongodb://sample-cluster.node.us-east-1.docdb.amazonaws.com:27017/
2018-11-14T17:21:18.516-0800 I NETWORK [thread1] getaddrinfo("sample-cluster.node.us-
east-1.docdb.amazonaws.com") failed:
nodename nor servname provided, or not known 2018-11-14T17:21:18.537-0800 E QUERY
 [thread1] Error: couldn't initialize
```

```
connection to host sample-cluster.node.us-east-1.docdb.amazonaws.com, address is
 invalid :
connect@src/mongo/shell/mongo.js:237:13@(connect):1:6
exception: connect failed
```

Para obtener el punto de conexión válido de un clúster, utilice el comando siguiente:

```
aws docdb describe-db-clusters \
   --db-cluster-identifier sample-cluster \
   --query 'DBClusters[*].[Endpoint,Port]'
```

Para obtener el punto de conexión válido de una instancia, utilice el comando siguiente:

```
aws docdb describe-db-instances \
   --db-instance-identifier sample-instance \
   --query 'DBInstances[*].[Endpoint.Address,Endpoint.Port]'
```

Para obtener más información, consulte Descripción de los puntos de conexión de Amazon DocumentDB.

La configuración del controlador afecta al número de conexiones

Al utilizar el controlador de cliente para conectarse a un clúster de Amazon DocumentDB, es importante tener en cuenta el parámetro de configuración `maxPoolSize`. La configuración `maxPoolSize` determina el número máximo de conexiones que el controlador de cliente mantendrá en su grupo de conexiones.

Índices de solución de problemas

En los temas siguientes, se explica lo que debe hacer si se produce un error durante la creación de un índice o un índice en segundo plano.

Temas

- Error al crear un índice
- El índice en segundo plano genera problemas de latencia y falla
- Sobrecarga del índice de base de datos

Error al crear un índice

Amazon DocumentDB utiliza el almacenamiento local de una instancia durante el proceso de creación de índices. Puede monitorizar este uso de disco mediante la métrica FreeLocalStorage de (`CloudWatch -> Metrics -> DocDB -> Instance Metrics`). Cuando la generación de un índice consume todo el espacio del disco local y no finaliza, se muestra un error. Cuando migre datos a Amazon DocumentDB, conviene que cree los índices primero y, a continuación, inserte los datos. Para obtener más información sobre las estrategias de migración y la creación de índices, consulte Migración a Amazon DocumentDB en la documentación de Amazon DocumentDB y la entrada de blog: Migrar de MongoDB a Amazon DocumentDB utilizando el método sin conexión.

Cuando cree índices en un clúster existente, si la creación del índice tarda más de lo previsto o no se realiza correctamente, le recomendamos que aumente el tamaño de la instancia para crear el índice y que, una vez creado, reduzca el tamaño. Amazon DocumentDB le permite escalar rápidamente los tamaños de las instancias en cuestión de minutos utilizando la Consola de administración de AWS o la AWS CLI. Para obtener más información, consulte Administración de clases de instancias. Dado que los precios de las instancias se calculan por segundos, solo pagará por los segundos en que esté utilizando los recursos.

El índice en segundo plano genera problemas de latencia y falla

Las compilaciones de índices en segundo plano en Amazon DocumentDB no se inician hasta que todas las consultas de la instancia principal que se iniciaron antes de que se iniciara la creación del índice terminen de ejecutarse. Si hay una consulta de larga duración, las compilaciones de índices en segundo plano se bloquearán hasta que finalice la consulta y, por lo tanto, pueden tardar más de lo esperado en completarse. Esto es válido incluso si las colecciones están vacías.

Las compilaciones de índices en primer plano no muestran el mismo comportamiento de bloqueo. En cambio, las compilaciones de índices en primer plano controlan exclusivamente la colección hasta que se complete la creación del índice. Por lo tanto, para crear índices en una colección vacía y evitar el bloqueo de consultas de larga duración, le sugerimos que utilice compilaciones de índices en primer plano.

> **Note**
>
> Amazon DocumentDB solo permite una operación de creación de índice en segundo plano en una colección al mismo tiempo. Si se producen operaciones de DDL (Lenguaje de

definición de datos) como `createIndex()` o `dropIndex()` en la misma colección durante la operación de creación de un índice en segundo plano, esta operación producirá un error.

Sobrecarga del índice de base de datos

Amazon DocumentDB utiliza el control de concurrencia multiversión (MVCC) para gestionar las transacciones simultáneas. Cuando los documentos se eliminan o actualizan, sus versiones anteriores permanecen en las colecciones e índices como versiones «inactivas». El proceso de recopilación de elementos no utilizados recupera automáticamente el espacio de estas versiones inactivas para futuras operaciones.

La sobrecarga de índices se produce cuando el tamaño de los índices de una colección aumenta debido a la acumulación de índices inactivos u obsoletos o a la fragmentación de las páginas. El porcentaje informado representa la cantidad de espacio de índice que pueden utilizar las entradas de índice futuras. Esta sobrecarga consume espacio tanto en la memoria caché como en el almacenamiento del búfer. Si desea eliminar la sobrecarga, tendrá que recopilar los índices.

Example Ejemplo

Ejecute el siguiente comando para determinar el almacenamiento no utilizado del índice:

```
db.coll.aggregate({$indexStats:{}});
```

El resultado tendrá un aspecto parecido al siguiente:

```
{
    "name" : "_id_",
    "key" : {
        "_id" : 1
    },
    "host" : "devbox-test.localhost.a2z.com:27317",
    "size" : NumberLong(827392),
    "accesses" : {
        "ops" : NumberLong(40000),
        "docsRead" : NumberLong(46049),
        "since" : ISODate("2025-04-03T21:44:51.251Z")
    },
    "cacheStats" : {
        "blksRead" : NumberLong(264),
        "blksHit" : NumberLong(140190),
```

```
        "hitRatio" : 99.8121
    },
    "unusedStorageSize" : {
        "unusedSizeBytes" : 409600,
        "unusedSizePercent" : 49.51
    }
}
```

Puede reconstruir los índices sin tiempo de inactividad mediante el comando `reIndex`, que requiere escanear toda la colección. Consulte Mantenimiento de índices mediante `reIndex`.

Solución de problemas de rendimiento y utilización de recursos

En esta sección se proporcionan preguntas y soluciones para los problemas de diagnóstico frecuentes en las implementaciones de Amazon DocumentDB. Los ejemplos que se proporcionan utilizan el shell de mongo y se limitan a una instancia individual. Para encontrar un punto de conexión de instancia, consulte Descripción de los puntos de conexión de Amazon DocumentDB.

Temas

- ¿Cómo determino el número de operaciones de inserción, actualización y eliminación realizadas en mi colección a través de la API de Mongo?
- ¿Cómo analizo el rendimiento de la memoria caché?
- ¿Cómo puedo encontrar y terminar las consultas que tardan mucho en ejecutarse o se bloquean?
- ¿Cómo puedo ver un plan de consulta y optimizar una consulta?
- ¿Cómo puedo ver un plan de consultas en clústeres elásticos?
- ¿Cómo puedo ver todas las operaciones en ejecución en una instancia?
- ¿Cómo sé cuándo una consulta está avanzando?
- ¿Cómo determino por qué de repente un sistema se ejecuta lentamente?
- ¿Cómo determino la causa del uso elevado de la CPU en una o varias instancias de clúster?
- ¿Cómo determino los cursores abiertos en una instancia?
- ¿Cómo determino la versión actual del motor de Amazon DocumentDB?
- ¿Cómo analizo el uso de los índices e identifico los índices no utilizados?
- ¿Cómo identifico los índices que faltan?
- ¿Cómo determino la sobrecarga de colecciones de bases de datos?
- Resumen de consultas útiles

¿Cómo determino el número de operaciones de inserción, actualización y eliminación realizadas en mi colección a través de la API de Mongo?

Para ver el número de operaciones de inserción, actualización y eliminación realizadas en una colección determinada, ejecute el siguiente comando en esa colección:

```
db.collection.stats()
```

La salida de este comando describe lo siguiente en su campo `opCounters`:

- numDocsIns: el número de documentos insertados en esta colección. Incluye los documentos insertados mediante los comandos `insert` y `insertMany`, así como los documentos insertados mediante actualizar o insertar.
- numDocsUpd: el número de documentos actualizados en esta colección. Incluye los documentos actualizados mediante los comandos `update` y `findAndModify`.
- numDocsDel: el número de documentos eliminados de esta colección. Incluye los documentos eliminados mediante los comandos `deleteOne`, `deleteMany`, `remove` y `findAndModify`.
- lastReset: hora a la que se restablecieron estos contadores por última vez. Las estadísticas proporcionadas por este comando se restablecen al iniciar o detener el clúster o al escalar la instancia en dirección ascendente o descendente.

A continuación, se muestra una salida de ejemplo de ejecución de `db.collection.stats()`.

```
{
    "ns" : "db.test",
    "count" : ...,
    "size" : ...,
    "avgObjSize" : ...,
    "storageSize" : ...,
    "capped" : false,
    "nindexes" : ...,
    "totalIndexSize" : ...,
    "indexSizes" : {
        "_id_" : ...,
        "x_1" : ...
    },
    "collScans" : ...,
    "idxScans" : ...,
```

```
    "opCounter" : {
        "numDocsIns" : ...,
        "numDocsUpd" : ...,
        "numDocsDel" : ...
    },
    "cacheStats" : {
        "collBlksHit" : ...,
        "collBlksRead" : ..,
        "collHitRatio" : ...,
        "idxBlksHit" : ...,
        "idxBlksRead" : ...,
        "idxHitRatio" : ...
    },
    "lastReset" : "2022-09-02 19:41:40.471473+00",
    "ok" : 1,
    "operationTime" : Timestamp(1662159707, 1)
}
```

Este comando de estadística debe usarse al ver los contadores específicos de la colección para las operaciones de inserción, actualización y eliminación a través de la API de Mongo. Otra forma de ver los contadores de operaciones específicas de una colección es habilitar la auditoría de DML. Se puede ver en Supervisión de Amazon DocumentDB con CloudWatch el número de operaciones de inserción, actualización y eliminación en todas las colecciones durante intervalos de un minuto.

¿Cómo analizo el rendimiento de la memoria caché?

El análisis del rendimiento de la memoria caché puede proporcionar información sobre la eficiencia de la recuperación de datos y el rendimiento del sistema, y se basa en la cantidad de datos que se leen del disco en comparación con la memoria caché. Proporcionamos estadísticas de la memoria caché sobre el número de visitas a la memoria caché (datos leídos de la memoria caché) y pérdidas de memoria caché (datos que no se encuentran en la memoria caché y se leen en el disco) para obtener información sobre el rendimiento de la memoria caché. Las estadísticas de la memoria caché de una colección específica se pueden encontrar ejecutando el siguiente comando en esa colección:

```
db.collection.stats()
```

Los valores del campo `cacheStats` del resultado de este comando proporcionan las estadísticas de la memoria caché de la colección, así como las estadísticas de la memoria caché totales de los índices creados en la colección. Estas estadísticas se muestran a continuación:

- **collBlksHit**: el número de bloques leídos de la memoria caché durante las operaciones de esta colección.
- **collBlksRead**: el número de bloques leídos del disco (pérdidas de memoria caché) durante las operaciones de esta colección.
- **collHitRatio**: la proporción de aciertos de la memoria caché de esta colección (`100 * [collBlksHit / (collBlksHit + collBlksRead)]`).
- **idxBlksHit**: el número de bloques leídos de la memoria caché para cualquier índice creado en esta colección.
- **idxBlksRead**: el número de bloques leídos del disco (pérdidas de memoria caché) para cualquier índice creado en esta colección.
- **idxHitRatio**: la proporción de aciertos de la memoria caché creados en esta colección (`100 * [idxBlksHit / (idxBlksHit + idxBlksRead)]`).
- **lastReset**: hora a la que se restablecieron estas estadísticas por última vez. Las estadísticas proporcionadas por `db.collection.stats()` se restablecen al iniciar o detener el clúster o al escalar la instancia en dirección ascendente o descendente.

También se puede encontrar un desglose de los campos `idxBlksHit` y `idxBlksRead` de cada índice mediante el comando `indexStats`. Puede encontrar las estadísticas de memoria caché específicas del índice ejecutando el siguiente comando:

```
db.collection.aggregate([{$indexStats:{}}]).pretty()
```

Para cada índice, se encuentran las siguientes estadísticas de memoria caché en el campo `cacheStats`:

- **blksHit**: el número de bloques leídos de la memoria caché para este índice.
- **blksRead**: el número de bloques leídos del disco para este índice.
- **blksHitRatio**: la proporción de aciertos de la memoria caché redondeada a cuatro decimales, calculada mediante `100 * [blksHit / (blksHit + blksRead)]`.

¿Cómo puedo encontrar y terminar las consultas que tardan mucho en ejecutarse o se bloquean?

Es posible que las consultas del usuario se ejecuten lentamente debido a que el plan de consultas es inadecuado o a que se bloquean debido a la contención de recursos.

Para buscar consultas de ejecución prolongada que se ralenticen a causa de un plan de consultas inadecuado o consultas que se bloquean debido a la contención de recursos, utilice el comando `currentOp`. Puede filtrar el comando para acotar la lista de las consultas relevantes que deben terminarse. Debe tener asociado `opid` a la consulta de ejecución prolongada para poder terminarla.

En la siguiente consulta, se utiliza el comando `currentOp` para ver todas las consultas que están bloqueadas o que se llevan ejecutando durante más de 10 segundos.

```
db.adminCommand({
    aggregate: 1,
    pipeline: [
        {$currentOp: {}},
        {$match:
            {$or: [
                {secs_running: {$gt: 10}},
                {WaitState: {$exists: true}}]}},
        {$project: {_id:0, opid: 1, secs_running: 1}}],
    cursor: {}
});
```

A continuación, puede limitar la consulta para encontrar el `opid` de una consulta que lleva ejecutándose durante más de 10 segundos y terminarla.

Para encontrar y terminar una consulta que lleva ejecutándose durante más de 10 segundos

1. Busque el `opid` de la consulta.

   ```
   db.adminCommand({
       aggregate: 1,
       pipeline: [
           {$currentOp: {}},
           {$match:
               {$or:
                   [{secs_running: {$gt: 10}},
                    {WaitState: {$exists: true}}]}}],
   ```

```
    cursor: {}
});
```

La salida de esta operación será similar a lo que se indica a continuación (formato JSON).

```
{
    "waitedMS" : NumberLong(0),
    "cursor" : {
        "firstBatch" : [
            {
                "opid" : 24646,
                "secs_running" : 12
            }
        ],
        "id" : NumberLong(0),
        "ns" : "admin.$cmd"
    },
    "ok" : 1
}
```

2. Termine la consulta con la operación `killOp`.

```
db.adminCommand({killOp: 1, op: 24646});
```

¿Cómo puedo ver un plan de consulta y optimizar una consulta?

Si una consulta se ejecuta lentamente, podría deberse a que la ejecución de la consulta requiere un examen completo de la colección para elegir los documentos pertinentes. A veces, la creación de los índices adecuados permite que la consulta se ejecute con mayor rapidez. Para detectar este escenario y decidir en qué campos se deben crear los índices, utilice el comando `explain`.

> **Note**
>
> Amazon DocumentDB emula la API MongoDB 3.6 en un motor de base de datos personalizada específicamente que utiliza un sistema de almacenamiento distribuido, tolerante a fallos y de recuperación automática. Como resultado, los planes de consulta y la salida de `explain()` pueden diferir entre Amazon DocumentDB y MongoDB. Los clientes que deseen controlar su plan de consulta pueden utilizar el operador `$hint` para aplicar la selección de un índice preferido.

Ejecute la consulta que desee mejorarse en el comando `explain` del modo siguiente.

```
db.runCommand({explain: {<query document>}})
```

A continuación se muestra un ejemplo de operación.

```
db.runCommand({explain:{
    aggregate: "sample-document",
    pipeline: [{$match: {x: {$eq: 1}}}],
    cursor: {batchSize: 1}}
});
```

La salida de esta operación será similar a lo que se indica a continuación (formato JSON).

```
{
    "queryPlanner" : {
        "plannerVersion" : 1,
        "namespace" : "db.test",
        "winningPlan" : {
            "stage" : "COLLSCAN"
        }
    },
    "serverInfo" : {
        "host" : "...",
        "port" : ...,
        "version" : "..."
    },
    "ok" : 1
}
```

El resultado anterior indica que la etapa `$match` requiere examinar todas las colecciones y comprobar si el campo `"x"` de cada documento es igual a 1. Si hay muchos documentos en la colección, el examen de la consulta (y, por tanto, el rendimiento general de la consulta) es muy lento. Por consiguiente, la presencia de `"COLLSCAN"` en el resultado del comando `explain` indica que el rendimiento de la consulta se puede mejorar creando los índices adecuados.

En este ejemplo, la consulta comprueba si el campo `"x"` es igual a 1 en todos los documentos. Por tanto, la creación de un índice en el campo `"x"` permite que la consulta evite el examen completo de la colección y utilice el índice para devolver los documentos pertinentes antes.

Después de crear un índice en el campo `"x"`, el resultado de `explain` es el siguiente.

```
{
    "queryPlanner" : {
         "plannerVersion" : 1,
         "namespace" : "db.test",
         "winningPlan" : {
             "stage" : "IXSCAN",
             "indexName" : "x_1",
             "direction" : "forward"
         }
    },
    "serverInfo" : {
        "host" : "...",
        "port" : ...,
        "version" : "..."
    },
    "ok" : 1
}
```

La creación de un índice en el campo `"x"` permite que la etapa `$match` utilice un análisis de índices para reducir el número de documentos en los que debe evaluarse el predicado `"x = 1"`.

En colecciones pequeñas, el procesador de consultas de Amazon DocumentDB puede optar por no utilizar un índice si las ventajas para el rendimiento son insignificantes.

¿Cómo puedo ver un plan de consultas en clústeres elásticos?

Para examinar un plan de consultas en clústeres elásticos, utilice el comando `explain`. A continuación, se muestra un ejemplo de operación `explain` en una consulta de búsqueda dirigida a una colección con partición:

```
db.runCommand(
   {
     explain: { find: "cities", filter: {"name": "Seoul"}}
   }
)
```

> **Note**
>
> Amazon DocumentDB emula MongoDB en un motor de base de datos personalizada. Como resultado, los planes de consulta y la salida de `explain()` pueden diferir entre Amazon

DocumentDB y MongoDB. Los clientes que deseen controlar su plan de consulta pueden utilizar el operador `$hint` para aplicar la selección de un índice preferido.

La salida de esta operación será similar a lo que se indica a continuación (formato JSON):

```
{
  "queryPlanner" : {
    "elasticPlannerVersion" : 1,
    "winningPlan" : {
      "stage" : "SINGLE_SHARD",
      "shards" : [
        {
          "plannerVersion" : 1,
          "namespace" : "population.cities",
          "winningPlan" : {
            "stage" : "SHARD_MERGE",
            "shards" : [
              {
                "shardName" : "f2cf5cfd-fe9c-40ca-b4e5-298ca0d11111",
                "plannerVersion" : 1,
                "namespace" : "population.cities",
                "winningPlan" : {
                  "stage" : "PARTITION_MERGE",
                  "inputStages" : [
                    {
                      "stage" : "COLLSCAN",
                      "partitionCount" : 21
                    }
                  ]
                }
              },
              {
                "shardName" : "8f3f80e2-f96c-446e-8e9d-aab8c7f22222",
                "plannerVersion" : 1,
                "namespace" : "population.cities",
                "winningPlan" : {
                  "stage" : "PARTITION_MERGE",
                  "inputStages" : [
                    {
                      "stage" : "COLLSCAN",
                      "partitionCount" : 21
                    }
```

```
                ]
              }
            },
            {
              "shardName" : "32c5a06f-1b2b-4af1-8849-d7c4a033333",
              "plannerVersion" : 1,
              "namespace" : "population.cities",
              "winningPlan" : {
                "stage" : "PARTITION_MERGE",
                "inputStages" : [
                  {
                    "stage" : "COLLSCAN",
                    "partitionCount" : 22
                  }
                ]
              }
            }
          ]
        },
        "shardName" : "32c5a06f-1b2b-4af1-8849-d7c4a0f3fb58"
      }
    ]
  }
},
"serverInfo" : {
  "host" : "example-4788267630.us-east-1.docdb-elastic.amazonaws.com:27017",
  "version" : "5.0.0"
},
"ok" : 1,
"operationTime" : Timestamp(1695097923, 1)
}
```

El resultado anterior muestra el plan de consulta para la consulta `find` en un clúster de tres particiones. Cada partición tiene varias particiones de datos que pueden tener diferentes etapas de entrada. En este ejemplo, se ejecuta un “COLLSCAN” (un escaneo de colecciones) en todas las particiones antes de fusionar los resultados en la etapa “PARTITION_MERGE” de cada partición. A continuación, los resultados de las particiones se combinan en la etapa “SHARD_MERGE” antes de enviarlos de vuelta al cliente.

¿Cómo puedo ver todas las operaciones en ejecución en una instancia?

Como un usuario o usuario principal, a menudo desea ver una lista de todas las operaciones que se están ejecutando actualmente en una instancia con fines de diagnóstico y para solucionar problemas. (Para obtener información acerca de cómo administrar los usuarios, consulte). Administración de usuarios de Amazon DocumentDB.)

Con el shell de mongo, puede utilizar la siguiente consulta para ver una lista de todas las operaciones en ejecución en una instancia de Amazon DocumentDB.

```
db.adminCommand({currentOp: 1, $all: 1});
```

La consulta devuelve la lista completa de todas las consultas del usuario y las tareas internas del sistema que se están realizando actualmente en la instancia.

La salida de esta operación será similar a lo que se indica a continuación (formato JSON).

```
{
    "inprog" : [
        {
            "desc" : "INTERNAL"
        },
        {
            "desc" : "TTLMonitor",
            "active" : false
        },
        {
            "client" : ...,
            "desc" : "Conn",
            "active" : true,
            "killPending" : false,
            "opid" : 195,
            "ns" : "admin.$cmd",
            "command" : {
                "currentOp" : 1,
                "$all" : 1
            },
            "op" : "command",
            "$db" : "admin",
            "secs_running" : 0,
            "microsecs_running" : NumberLong(68),
```

```
            "clientMetaData" : {
            "application" : {
                "name" : "MongoDB Shell"
            },
            "driver" : {
                ...
            },
            "os" : {
                ...
            }
          }
       },
       {
          "desc": "GARBAGE_COLLECTION",
          "garbageCollection": {
             "databaseName": "testdb",
             "collectionName": "testCollectionA"
          },
          "secs_running": 3,
          "microsecs_running": NumberLong(3123456)
       },
       {
          "desc": "GARBAGE_COLLECTION",
          "garbageCollection": {
             "databaseName": "testdb",
             "collectionName": "testCollectionB"
          },
          "secs_running": 4,
          "microsecs_running": NumberLong(4123456)
       }
    ],
    "ok" : 1
}
```

Los siguientes valores son válidos para el campo `"desc"`:

- **`INTERNAL`**: tareas internas del sistema, como tareas de limpieza del cursor o limpieza de usuarios obsoletos.
- **`TTLMonitor`**: el hilo de supervisión de tiempo de vida (TTL). Su estado de funcionamiento se refleja en el campo `"active"`.
- **`GARBAGE_COLLECTION`**: el subproceso del recolector de elementos no utilizados interno.
- **`CONN`**: la consulta del usuario.

- **`CURSOR`**: la operación consiste en un cursor inactivo que espera a que el usuario ejecute el comando “GetMore” para obtener el siguiente lote de resultados. En este estado, el cursor consume memoria, pero no consume capacidad de cálculo.

El resultado anterior también muestra todas las consultas del usuario que se ejecutan en el sistema. Cada consulta del usuario se ejecuta en el contexto de una base de datos y una colección. La unión de las dos se denomina espacio de nombres. El espacio de nombres de cada consulta del usuario está disponible en el campo `"ns"`.

A veces, es necesario ver una lista de todas las consultas del usuario que se están ejecutando en un determinado espacio de nombres. Por tanto, el resultado anterior debe filtrarse en el campo `"ns"`. A continuación, se muestra una consulta de ejemplo para conseguir el resultado que se va a filtrar. La consulta muestra todas las consultas del usuario que se están ejecutando actualmente en la base de datos `"db"` y la colección `"test"` (es decir, el espacio de nombres `"db.test"`).

```
db.adminCommand({aggregate: 1,
    pipeline: [{$currentOp: {allUsers: true, idleConnections: true}},
               {$match: {ns: {$eq: "db.test"}}}],
    cursor: {}
});
```

Como usuario principal del sistema, puede ver las consultas de todos los usuarios y también todas las tareas internas del sistema. Los demás usuarios solo pueden ver sus consultas respectivas.

Si el número total de consultas y tareas internas del sistema supera el tamaño del cursor batch predeterminado, el shell de `mongo` genera automáticamente un objeto de iteración `'it'` para ver el resto de los resultados. Siga ejecutando el comando `'it'` hasta que se hayan agotado todos los resultados.

¿Cómo sé cuándo una consulta está avanzando?

Es posible que las consultas del usuario se ejecuten lentamente debido a que el plan de consultas es inadecuado o a que se bloquean debido a la contención de recursos. La depuración de estas consultas es un proceso de varios pasos en el que puede ser necesario realizar el mismo paso varias veces.

El primer paso de la depuración es mostrar todas las consultas que tardan mucho tiempo en ejecutarse o que se bloquean. La siguiente consulta muestra todas las consultas del usuario que se han ejecutado durante más de 10 segundos o que están esperando recursos.

```
db.adminCommand({aggregate: 1,
                 pipeline: [{$currentOp: {}},
                            {$match: {$or: [{secs_running: {$gt: 10}},
                                            {WaitState: {$exists: true}}]}},
                            {$project: {_id:0,
                                        opid: 1,
                                        secs_running: 1,
                                        WaitState: 1,
                                        blockedOn: 1,
                                        command: 1}}],
                 cursor: {}
                });
```

Repita la consulta anterior de forma periódica para determinar si la lista de consultas cambia e identificar la consulta de ejecución prolongada o las consultas bloqueadas.

Si el documento de salida de la consulta en cuestión tiene un campo `WaitState`, indica que la contención de recursos es la razón por la que la consulta tarda mucho en ejecutarse o se bloquea. La contención de recursos puede deberse a operaciones de E/S, tareas internas del sistema u otras consultas del usuario.

La salida de esta operación será similar a lo que se indica a continuación (formato JSON).

```
{
    "waitedMS" : NumberLong(0),
    "cursor" : {
        "firstBatch" : [
            {
                "opid" : 201,
                "command" : {
                    "aggregate" : ...
                },
                "secs_running" : 208,
                "WaitState" : "IO"
            }
        ],
        "id" : NumberLong(0),
        "ns" : "admin.$cmd"
    },
    "ok" : 1
}
```

Las operaciones de E/S pueden producir un cuello de botella si se ejecutan muchas consultas en diferentes colecciones al mismo tiempo en la misma instancia o si la instancia es demasiado pequeña para el conjunto de datos en el que se está ejecutando la consulta. Si las consultas son consultas de solo lectura, puede mitigar la situación anterior separando las consultas de cada colección en réplicas diferentes. En las actualizaciones simultáneas en diferentes colecciones o cuando el tamaño de la instancia es demasiado pequeño para el conjunto de datos, puede mitigarla ampliando la instancia.

Si la contención de recursos se debe a otras consultas del usuario, el campo `"blockedOn"` del documento de salida contendrá el `"opid"` de la consulta que afecta a esta consulta. Mediante el `"opid"`, siga la cadena de campos `"WaitState"` y `"blockedOn"` de todas las consultas para encontrar la consulta de la parte superior de la cadena.

Si la tarea de la parte superior de la cadena es una tarea interna, la única forma de mitigar este problema sería finalizar la consulta y volver a ejecutarla más adelante.

A continuación, se muestra un resultado de ejemplo en el que la consulta de búsqueda está bloqueada en un bloqueo de la colección propiedad de otra tarea.

```
{
    "inprog" : [
        {
            "client" : "...",
            "desc" : "Conn",
            "active" : true,
            "killPending" : false,
            "opid" : 75,
            "ns" : "...",
            "command" : {
                "find" : "...",
                "filter" : {

                }
            },
            "op" : "query",
            "$db" : "test",
            "secs_running" : 9,
            "microsecs_running" : NumberLong(9449440),
            "threadId" : 24773,
            "clientMetaData" : {
                "application" : {
                   "name" : "MongoDB Shell"
```

```
                },
                "driver" : {
                    ...
                },
                "os" : {
                    ...
                }
            },
            "WaitState" : "CollectionLock",
            "blockedOn" : "INTERNAL"
        },
        {
            "desc" : "INTERNAL"
        },
        {
            "client" : "...",
            ...
            "command" : {
                "currentOp" : 1
            },
            ...
        }
    ],
    "ok" : 1
}
```

Si `"WaitState"` tiene los valores `"Latch"`, `"SystemLock"`, `"BufferLock"`, `"BackgroundActivity"` o `"Other"`, la contención de recursos se debe a tareas internas del sistema. Si la situación continúa durante mucho tiempo, la única forma de mitigar este problema sería finalizar la consulta y volver a ejecutarla más adelante.

¿Cómo determino por qué de repente un sistema se ejecuta lentamente?

A continuación, se indican algunos motivos frecuentes de la ralentización del sistema:

- Contención excesiva de recursos entre consultas simultáneas
- El número de consultas simultáneas activas aumenta con el tiempo
- Tareas internas del sistema como `"GARBAGE_COLLECTION"`

Para monitorizar el uso del sistema a lo largo del tiempo, ejecute la siguiente consulta `"currentOp"` periódicamente y envíe los resultados a un almacén externo. La consulta cuenta la cantidad de

consultas y operaciones en cada espacio de nombres del sistema. A continuación, puede analizar los resultados de uso del sistema para conocer la carga del sistema y tomar las medidas adecuadas.

```
db.adminCommand({aggregate: 1,
                 pipeline: [{$currentOp: {allUsers: true, idleConnections: true}},
                            {$group: {_id: {desc: "$desc", ns: "$ns", WaitState:
 "$WaitState"}, count: {$sum: 1}}}],
                 cursor: {}
                });
```

Esta consulta devuelve la suma de todas las consultas que se ejecutan en cada espacio de nombres, todas las tareas internas del sistema y el número único de estados de espera (si hay alguno) por espacio de nombres.

La salida de esta operación será similar a lo que se indica a continuación (formato JSON).

```
{
    "waitedMS" : NumberLong(0),
    "cursor" : {
        "firstBatch" : [
            {
                "_id" : {
                    "desc" : "Conn",
                    "ns" : "db.test",
                    "WaitState" : "CollectionLock"
                },
               "count" : 2
            },
            {
                "_id" : {
                    "desc" : "Conn",
                    "ns" : "admin.$cmd"
                },
                "count" : 1
            },
            {
                "_id" : {
                    "desc" : "TTLMonitor"
                },
                "count" : 1
            }
        ],
```

```
        "id" : NumberLong(0),
        "ns" : "admin.$cmd"
    },
    "ok" : 1
}
```

En el resultado anterior, hay dos consultas de usuario en el espacio de nombres `"db.test"` que están bloqueadas en el bloqueo de colección: una consulta en el espacio de nombres `"admin.$cmd"` y una tarea interna `"TTLMonitor"`.

Si el resultado indica muchas consultas con estados de espera de bloqueo, consulte ¿Cómo puedo encontrar y terminar las consultas que tardan mucho en ejecutarse o se bloquean?

¿Cómo determino la causa del uso elevado de la CPU en una o varias instancias de clúster?

Las secciones siguientes pueden ayudarle a identificar la causa del uso elevado de la CPU en una instancia. Los resultados pueden variar en función de la carga de trabajo.

- Para determinar por qué una instancia de repente se ejecuta lentamente, consulte ¿Cómo determino por qué de repente un sistema se ejecuta lentamente?
- Para identificar y terminar consultas de ejecución largas en una instancia determinada, consulte ¿Cómo puedo encontrar y terminar las consultas que tardan mucho en ejecutarse o se bloquean?
- Para saber si una consulta avanza, consulte ¿Cómo sé cuándo una consulta está avanzando?
- Para determinar por qué una consulta tarda mucho tiempo en ejecutarse, consulte ¿Cómo puedo ver un plan de consulta y optimizar una consulta?
- Para realizar un seguimiento de las consultas de ejecución prolongada con el tiempo, consulte Creación de perfiles de operaciones en Amazon DocumentDB.

En función del motivo del uso elevado de la CPU en la instancia, puede resultar útil realizar una o varias de las siguientes acciones.

- Si la instancia principal presenta un uso elevado de la CPU, pero las instancias de réplica no, considere la posibilidad de distribuir el tráfico de lectura entre las réplicas a través de la configuración de preferencia de lectura del cliente (por ejemplo, `secondaryPreferred`). Para obtener más información, consulte Conexión a Amazon DocumentDB como conjunto de réplicas.

Si se utilizan réplicas para las lecturas, se puede aprovechar mejor los recursos del clúster permitiendo que la instancia principal procese más tráfico de escritura. Las lecturas de las réplicas presentan consistencia final.

- Si el uso elevado de la CPU se debe a la carga de trabajo de escritura, cambiar el tamaño de las instancias del clúster a un tipo de instancia mayor aumenta el número de núcleos de la CPU disponibles para atender la carga de trabajo. Para obtener más información, consulte instancias y Especificaciones de clases de instancias.
- Si todas las instancias del clúster presentan un uso elevado de la CPU y la carga de trabajo utiliza réplicas para las lecturas, añadir más réplicas al clúster aumenta los recursos disponibles para el tráfico de lectura. Para obtener más información, consulte Agregación de una instancia de Amazon DocumentDB a un clúster.

¿Cómo determino los cursores abiertos en una instancia?

Cuando está conectado a una instancia Amazon DocumentDB, puede utilizar el comando `db.runCommand("listCursors")` para enumerar los cursores abiertos en esa instancia. Hay un límite de hasta 4560 cursores activos abiertos en un momento dado en una instancia determinada de Amazon DocumentDB, según el tipo de instancia. Por lo general, se recomienda cerrar cursores que ya no están en uso porque los cursores utilizan recursos en una instancia y tienen un límite superior. Consulte en Cuotas y límites de Amazon DocumentDB los límites específicos.

```
db.runCommand("listCursors")
```

¿Cómo determino la versión actual del motor de Amazon DocumentDB?

Para determinar la versión actual del motor de Amazon DocumentDB, ejecute el siguiente comando.

```
db.runCommand({getEngineVersion: 1})
```

La salida de esta operación será similar a lo que se indica a continuación (formato JSON).

```
{ "engineVersion" : "2.x.x", "ok" : 1 }
```

> **Note**
>
> La versión de motor de Amazon DocumentDB 3.6 es 1.x.x y la versión de motor de Amazon DocumentDB 4.0 es 2.x.x.

¿Cómo analizo el uso de los índices e identifico los índices no utilizados?

Para identificar los índices de una colección determinada, ejecute el siguiente comando:

```
db.collection.getIndexes()
```

Para analizar cuántos índices se utilizan durante las operaciones realizadas en las colecciones, se pueden utilizar los comandos `collStats` y `indexStats`. Para ver el número total de escaneos realizados con índices (escaneos de índices) en comparación con el número de escaneos realizados sin un índice (escaneos de colecciones), ejecute el siguiente comando:

```
db.collection.stats()
```

El resultado de este comando incluye los valores que se muestran a continuación:

- **`idxScans`**: el número de escaneos realizados en esta colección mediante un índice.
- **`collScans`**: el número de escaneos realizados en esta colección sin un índice. Estos escaneos habrían implicado revisar los documentos de la colección uno por uno.
- **`lastReset`**: hora a la que se restablecieron estos contadores por última vez. Las estadísticas proporcionadas por este comando se restablecen al iniciar o detener el clúster o al escalar la instancia en dirección ascendente o descendente.

En el resultado del siguiente comando se muestra un desglose del uso de cada índice. Es una práctica recomendada identificar y eliminar regularmente los índices no utilizados para mejorar el rendimiento y reducir los costos, ya que de esta forma se eliminan las operaciones informáticas, de almacenamiento y de E/S innecesarias utilizadas para mantener los índices.

```
db.collection.aggregate([{$indexStats:{}}]).pretty()
```

El resultado de este comando proporciona los siguientes valores para cada índice creado en la colección:

- **`ops`**: el número de operaciones que utilizaron el índice. Si la carga de trabajo se ha ejecutado durante un tiempo suficientemente largo y está seguro de que se encuentra en un estado estable, un valor `ops` de cero indicaría que el índice no se utiliza en absoluto.
- **`numDocsRead`**: el número de documentos leídos durante las operaciones que utilizan este índice.
- **`since`**: el tiempo transcurrido desde que Amazon DocumentDB comenzó a recopilar estadísticas sobre el uso del índice, que suele ser el valor transcurrido desde la última acción de reinicio o mantenimiento de la base de datos.
- **`size`**: tamaño de este archivo en bytes.

El siguiente ejemplo es una muestra del resultado de ejecutar el comando anterior:

```
{
    "name" : "_id_",
    "key" : {
        "_id" : 1
    },
    "host" : "example-host.com:12345",
    "size" : NumberLong(...),
    "accesses" : {
        "ops" : NumberLong(...),
        "docsRead" : NumberLong(...),
        "since" : ISODate("...")
    },
    "cacheStats" : {
        "blksRead" : NumberLong(...),
        "blksHit" : NumberLong(...),
        "hitRatio" : ...
    }
}
{
    "name" : "x_1",
    "key" : {
        "x" : 1
    },
    "host" : "example-host.com:12345",
    "size" : NumberLong(...),
    "accesses" : {
        "ops" : NumberLong(...),
        "docsRead" : NumberLong(...),
        "since" : ISODate("...")
    },
```

```
    "cacheStats" : {
        "blksRead" : NumberLong(...),
        "blksHit" : NumberLong(...),
        "hitRatio" : ...
    }
}
```

Para determinar el tamaño del índice general de una colección, ejecute el siguiente comando:

```
db.collection.stats()
```

Para eliminar un índice no utilizado, ejecute el siguiente comando:

```
db.collection.dropIndex("indexName")
```

¿Cómo identifico los índices que faltan?

Puede utilizar el generador de perfiles de Amazon DocumentDB para registrar consultas lentas. Una consulta que aparece repetidamente en el registro de consultas lentas puede indicar que se requiere un índice adicional para mejorar el rendimiento de esa consulta.

Para identificar opciones de índices útiles, puede buscar consultas de larga duración que tengan una o más etapas que realicen al menos una etapa `COLLSCAN`, lo que significa que la etapa de consulta tiene que leer todos los documentos de la colección para proporcionar una respuesta a la consulta.

En el ejemplo siguiente se muestra una consulta en una colección de viajes en taxi que se ejecutaron en una colección grande.

```
db.rides.count({"fare.totalAmount":{$gt:10.0}}))
```

Para ejecutar este ejemplo, la consulta tuvo que realizar un análisis de la colección (es decir, leer cada documento de la colección), ya que no hay ningún índice en el campo `fare.totalAmount`. La salida del generador de perfiles de Amazon DocumentDB para esta consulta es similar a la siguiente:

```
{
    ...
    "cursorExhausted": true,
    "nreturned": 0,
    "responseLength": 0,
```

```
    "protocol": "op_query",
    "millis": 300679,
    "planSummary": "COLLSCAN",
    "execStats": {
        "stage": "COLLSCAN",
        "nReturned": "0",
        "executionTimeMillisEstimate": "300678.042"
    },
    "client": "172.31.5.63:53878",
    "appName": "MongoDB Shell",
    "user": "example"
}
```

Para acelerar la consulta de este ejemplo, crearía un índice en `fare.totalAmount`, como se muestra a continuación.

```
db.rides.createIndex( {"fare.totalAmount": 1}, {background: true} )
```

> **Note**
>
> Los índices creados en el primer caso (es decir, cuando la opción `{background:true}` no se proporciona al crear el índice) utilizan un bloqueo de escritura exclusivo, lo que impide que las aplicaciones escriban datos en la colección hasta que se completa la creación del índice. Tenga en cuenta este impacto potencial al crear índices en clústeres de producción. Al crear índices, recomendamos configurar `{background:true}`.

En general, le convendrá crear índices en campos que tengan una cardinalidad alta (por ejemplo, un gran número de valores únicos). Crear un índice en un campo con cardinalidad baja puede producir un índice grande que no se utilice. El optimizador de consultas de Amazon DocumentDB tiene en cuenta el tamaño general de la colección y la selectividad de los índices al crear un plan de consulta. Hay momentos en los que verá que el procesador de consultas selecciona una etapa `COLLSCAN` incluso cuando un índice está presente. Esto sucede cuando el procesador de consultas estima que la utilización del índice no ofrecerá una ventaja de rendimiento sobre el análisis de toda la colección. Si desea obligar a que el procesador de consultas utilice un índice en particular, puede utilizar el operador `hint()` como se muestra a continuación.

```
db.collection.find().hint("indexName")
```

¿Cómo determino la sobrecarga de colecciones de bases de datos?

La sobrecarga de colecciones se produce cuando el tamaño de una colección aumenta debido a la acumulación de documentos inactivos u obsoletos o a la fragmentación de las páginas de la base de datos. El porcentaje informado representa la cantidad de espacio de documento que pueden utilizar documentos futuros. Esta sobrecarga consume espacio tanto en la memoria caché como en el almacenamiento del búfer. Para eliminar la sobrecarga, las colecciones deben volver a cargarse mediante volcado/restauración o mediante un bucle de migración y una transición durante un período de mantenimiento.

Example Ejemplo

Ejecute el siguiente comando para determinar el almacenamiento no utilizado de la colección:

```
db.runCommand({collStats:'coll'})
```

El resultado tendrá un aspecto parecido al siguiente:

```
{
        "ns" : "test.coll",
        "count" : 7500,
        "size" : 23250,
        "avgObjSize" : 31,
        "storageSize" : 106496,
        "unusedStorageSize" : {
                "unusedBytes" : 16384,
                "unusedPercent" : 25.12
        },
        "compression" : {
                "enable" : false
        },
        "capped" : false,
        "nindexes" : 1,
        "totalIndexSize" : 57344,
        "indexSizes" : {
                "_id_" : 57344
        },
        "collScans" : 4,
        "idxScans" : 10000,
        "opCounter" : {
                "numDocsIns" : 1000,
                "numDocsUpd" : 0,
```

```
                "numDocsDel" : 250
        },
        "cacheStats" : {
                "collBlksHit" : 3570,
                "collBlksRead" : 8,
                "collHitRatio" : 99.7765,
                "idxBlksHit" : 12293,
                "idxBlksRead" : 6,
                "idxHitRatio" : 99.9513
        },
        "lastReset" : "2024-12-18 00:30:21.552019+00",
        "ok" : 1,
        "operationTime" : Timestamp(1734632375, 1)
}
```

Resumen de consultas útiles

Las siguientes consultas pueden resultar útiles para monitorizar el rendimiento y el uso de recursos en Amazon DocumentDB..

- Utilice el siguiente comando para ver las estadísticas de una colección específica, incluidos los contadores de operaciones, las estadísticas de memoria caché, las estadísticas de acceso y las estadísticas de tamaño:

  ```
  db.collection.stats()
  ```

- Utilice el siguiente comando para ver las estadísticas de cada índice creado en una colección, incluido el tamaño del índice, las estadísticas de caché específicas del índice y las estadísticas de uso del índice:

  ```
  db.collection.aggregate([{$indexStats:{}}]).pretty()
  ```

- Utilice la siguiente consulta para ver toda la actividad.

  ```
  db.adminCommand({currentOp: 1, $all: 1});
  ```

- El código siguiente muestra una lista de todas las consultas de ejecución prolongada o bloqueadas.

  ```
  db.adminCommand({aggregate: 1,
                   pipeline: [{$currentOp: {}},
  ```

```
                            {$match: {$or: [{secs_running: {$gt: 10}},
                                            {WaitState: {$exists: true}}]}},
                            {$project: {_id:0,
                                        opid: 1,
                                        secs_running: 1,
                                        WaitState: 1,
                                        blockedOn: 1,
                                        command: 1}}],
                 cursor: {}
                });
```

- El código siguiente finaliza una consulta.

```
db.adminCommand({killOp: 1, op: <opid of running or blocked query>});
```

- Utilice el código siguiente para obtener una vista acumulada del estado del sistema.

```
db.adminCommand({aggregate: 1,
                 pipeline: [{$currentOp: {allUsers: true, idleConnections: true}},
                            {$group: {_id: {desc: "$desc", ns: "$ns", WaitState:
 "$WaitState"}, count: {$sum: 1}}}],
                 cursor: {}
                });
```

Recopilación de elementos no utilizados en Amazon DocumentDB

Amazon DocumentDB implementa una arquitectura de base de datos de control de concurrencia multiversión (MVCC) que crea nuevas versiones de entradas de documentos e índices para cada operación de actualización. Esta arquitectura permite el aislamiento de las transacciones, evitando que los cambios de una transacción aparezcan en otra.

Temas

- Descripción de la recolección de basura en Amazon DocumentDB
- Proceso de recopilación de elementos no utilizados
- Arquitectura de almacenamiento y almacenamiento ampliado
- Supervisión de recopilación de elementos no utilizados
- Ejemplo de salida de CollStats
- Preguntas frecuentes

Descripción de la recolección de basura en Amazon DocumentDB

La recopilación de elementos no utilizados (GC) es un proceso en segundo plano automatizado que mantiene un rendimiento y una disponibilidad óptimos del sistema en Amazon DocumentDB. Al igual que muchas bases de datos modernas, la arquitectura MVCC de Amazon DocumentDB crea nuevas versiones de documentos e índices con cada actualización. Cada operación de escritura consume un identificador MVCC único de un contador finito. IDs Identifican a qué transacción pertenece una versión de un documento y si se ha confirmado o anulado. Con el tiempo, estas versiones antiguas y su MVCC IDs se acumulan y es necesario limpiarlas para evitar una degradación del rendimiento.

Funciones de la recopilación de elementos no utilizados

El recopilador de elementos no utilizados cumple tres funciones esenciales:

- Recupera espacio de almacenamiento: elimina las versiones obsoletas de documentos e índices que las consultas activas ya no necesitan, lo que libera espacio para futuras operaciones de escritura.
- Evita el desbordamiento de ID de MVCC: evita el desbordamiento de ID de MVCC mediante la gestión del contador finito de MVCC. IDs Sin esta administración, el contador eventualmente alcanzaría su límite, lo que obligaría a la base de datos a pasar a un modo temporal de solo lectura hasta que se recicle. IDs
- Mantiene el rendimiento de las consultas: mantiene un rendimiento óptimo de las consultas, ya que elimina las versiones inactivas de los documentos que, de otro modo, se acumularían y ralentizarían el procesamiento de las consultas.

Proceso de recopilación de elementos no utilizados

El proceso de GC funciona por colección y puede tener varios procesos ejecutándose simultáneamente en diferentes colecciones. El proceso consta de cuatro fases secuenciales:

1. Identificación: el sistema identifica las versiones de documentos e índices a las que ya no hacen referencia las transacciones ni consultas activas.
2. Carga de memoria: los documentos antiguos y las entradas del índice se cargan en la memoria si aún no están presentes.
3. Eliminación: las versiones obsoletas se eliminan permanentemente para recuperar espacio de almacenamiento.

4. Reciclaje de identificadores de MVCC: el sistema recicla los MVCC de las versiones eliminadas para utilizarlos en IDs nuevas operaciones.

Cuando la recolección de basura termina de procesar las versiones antiguas de los documentos, elimina el MVCC IDs más antiguo del sistema. Esta limpieza es fundamental para evitar que los identificadores de los MVCC se desborden IDs, ya que reciclan los MVCC y los ponen a disposición para nuevas operaciones de escritura en todo el clúster. Sin este proceso de reciclaje, el sistema acabaría agotando su contador finito de identificadores de MVCC y pasaría a un estado de solo lectura.

Programación de recopilación de elementos no utilizados

La recopilación de elementos no utilizados se ejecuta automáticamente en segundo plano a intervalos periódicos. La temporización y la frecuencia se ajustan dinámicamente en función de la carga del sistema, los recursos disponibles, el volumen de escritura y los niveles de consumo de los identificadores de MVCC. Cuando hay mucha actividad de escritura, el proceso de GC se ejecuta con más frecuencia para administrar el aumento del número de versiones de los documentos.

Arquitectura de almacenamiento y almacenamiento ampliado

Amazon DocumentDB utiliza una arquitectura de almacenamiento sofisticada que separa el almacenamiento de documentos en dos segmentos distintos:

Segmento de almacenamiento base

El segmento de almacenamiento base contiene los datos y metadatos del documento principal. Este segmento almacena:

- Contenido del documento que se ajusta al tamaño de página estándar (8 KB).
- Información de estructura y metadatos del documento.
- Índices principales y sus entradas.
- Estadísticas y configuración a nivel de colección.

Segmento de almacenamiento extendido

El segmento de almacenamiento ampliado utiliza un almacén de objetos de documentos de gran tamaño especializado diseñado para gestionar documentos que superan el tamaño de página de almacenamiento estándar. Este segmento ofrece:

- Gestión eficiente de documentos de gran tamaño: los documentos que superen el umbral de almacenamiento base se trasladan automáticamente al segmento de almacenamiento ampliado.
- Diseño de almacenamiento optimizado: el segmento utiliza un formato de almacenamiento diferente, optimizado para objetos de gran tamaño, lo que reduce la fragmentación y mejora los patrones de acceso.
- Recolección de basura independiente: el segmento de almacenamiento ampliado tiene su propio proceso de recolección de basura que puede ejecutarse independientemente de la limpieza del almacenamiento base.
- Acceso transparente: las aplicaciones acceden a documentos grandes sin problemas sin necesidad de saber qué segmento de almacenamiento contiene los datos.

El segmento de almacenamiento ampliado es particularmente beneficioso para:

- Colecciones con documentos que contienen matrices integradas de gran tamaño.
- Documentos con amplias estructuras anidadas.
- Colecciones que almacenan datos binarios o campos de texto de gran tamaño.
- Aplicaciones con documentos de distintos tamaños, en las que algunos documentos superan considerablemente el tamaño medio.

Supervisión de recopilación de elementos no utilizados

Métricas de nivel de clúster

`AvailableMVCCIds`

- Ubicación — Amazon CloudWatch
- Descripción: contador que muestra el número de operaciones de escritura restantes disponibles desde un límite máximo de 1800 millones. Cuando este contador llega a cero, el clúster pasa al modo de solo lectura hasta que IDs se recupere y se recicle. El contador disminuye con cada operación de escritura y aumenta a medida que la recolección de basura recicla el MVCC antiguo. IDs
- Recomendación: active una alarma cuando el valor disminuya por debajo de 1300 millones. Esta alerta temprana le permite tomar las medidas recomendadas que se describen más adelante.

`LongestActiveGCRuntime`

- Ubicación — Amazon CloudWatch
- Descripción: duración en segundos del proceso de recopilación de elementos no utilizados más prolongado. Se actualiza cada minuto y realiza un seguimiento únicamente de las operaciones activas, excluyendo los procesos que se completan en el intervalo de un minuto.
- Recomendación: Compárelos con los datos `gcRuntimeStats` históricos para identificar un comportamiento anormal en la recolección de basura, como los tiempos de ejecución prolongados durante las eliminaciones masivas.

Métricas a nivel de la colección

`MVCCIDStats: MVCCIdScale`

- Ubicación: comando collStats de la base de datos
- Descripción: mide la antigüedad del identificador de MVCC en una escala de 0 a 1, donde 1 indica la antigüedad máxima antes de que un clúster entre en estado de solo lectura. Utilice esta métrica `AvailableMVCCIds` para identificar las colecciones que contienen el MVCC más antiguo y IDs que están anticuadas en el clúster.
- Recomendación: mantenga los valores por debajo de 0,3 para cada colección.

`gcRuntimeStats`

- Ubicación: comando collStats de la base de datos
- Descripción: proporciona un historial de dos meses con las métricas de recopilación de elementos no utilizados, que incluye el total de ejecuciones, la duración promedio y la duración máxima. Solo incluye las operaciones de recopilación de elementos no utilizados que duren más de cinco minutos para garantizar estadísticas significativas.

> **Important**
>
> `gcRuntimeStatsdocumentFragmentStats`, y el desglose de las métricas a nivel de recopilación en Amazon DocumentDB `storageSegmentBase` 8.0 y solo `storageSegmentExtended` están disponibles para Amazon DocumentDB 8.0.

`storageSizeStats`

- Ubicación: comando collStats de la base de datos
- Descripción: proporciona un desglose detallado de la utilización del almacenamiento en los diferentes segmentos de almacenamiento:
  - `storageSegmentBase`— Almacenamiento utilizado por el segmento de almacenamiento base para documentos estándar
  - `storageSegmentExtended`— Almacenamiento utilizado por el segmento de almacenamiento ampliado para documentos de gran tamaño
- Uso: ayuda a identificar las colecciones con un almacenamiento de documentos de gran tamaño y a comprender los patrones de distribución del almacenamiento.

`unusedStorageSize` (nivel de colección)

- Ubicación: comando collStats de la base de datos
- Descripción: estima el espacio de almacenamiento no utilizado en una colección en función de las estadísticas muestreadas. Incluye el espacio de los documentos eliminados y de los segmentos vacíos. La métrica proporciona tanto los totales combinados como los desgloses por segmento:
  - Combinados `unusedBytes` y en `unusedPercent` todos los segmentos de almacenamiento
  - `storageSegmentBase`— Espacio no utilizado específicamente en el segmento de almacenamiento base
  - `storageSegmentExtended`— Espacio no utilizado específicamente en el segmento de almacenamiento ampliado

`documentFragmentStats`

- Ubicación: comando collStats de la base de datos
- Descripción: proporciona información detallada sobre los fragmentos de documentos y los datos inactivos de las colecciones. Los fragmentos de documentos representan las unidades de almacenamiento internas utilizadas por el motor de base de datos, y los fragmentos muertos indican datos a los que ya no se puede acceder pero que aún no se han recuperado. Esta métrica incluye:
  - `totalDocFragmentsCount`— Número total de fragmentos de documentos de la colección
  - `deadDocFragmentsCount`— Número de fragmentos que contienen datos muertos (inaccesibles)
  - `deadDocFragmentsPercent`— Porcentaje de fragmentos que contienen datos muertos

  - `deadDocFragmentBytes`— Número estimado de bytes consumidos por fragmentos de documentos muertos
  - Desglose por segmento para y `storageSegmentBase` `storageSegmentExtended`
- Uso: supervise esta métrica para comprender la eficacia de la recolección de basura e identificar las recolecciones que podrían beneficiarse de las operaciones de mantenimiento. Los altos porcentajes de fragmentos muertos indican que la recolección de basura puede estar retrasándose o que la recolección se beneficiaría de una optimización.

Métricas de nivel de índice

`unusedStorageSize` (nivel de índice)

- Ubicación: comando IndexStats de la base de datos.
- Descripción: estima el espacio de almacenamiento no utilizado en un índice en función de las estadísticas muestreadas. Incluye el espacio de las entradas de índice obsoletas y de los segmentos vacíos.
- Recomendación: utilice el comando `reIndex` para compilar los índices sin tiempo de inactividad y recuperar el espacio no utilizado. Consulte Administración de índices para obtener más detalles.

Ejemplo de salida de CollStats

El siguiente ejemplo muestra un `collStats` resultado típico con métricas de recolección y almacenamiento de basura:

```
{
    "ns" : "Mvcc_consumption_test_db.mvcc_test_collection",
    "MVCCIdStats" : {
        "MVCCIdScale" : 0.03
    },
    "gcRuntimeStats" : {
        "numRuns" : 1,
        "historicalAvgRuntime" : 3295,
        "historicalMaxRuntime" : 3295,
        "lastRuntime" : 3295,
        "lastRuntimeStart" : ISODate("2025-06-24T08:47:14Z")
    },
    "documentFragmentStats" : {
        "totalDocFragmentsCount" : 45000000,
```

```
        "deadDocFragmentsCount" : 2250000,
        "deadDocFragmentsPercent" : 5.0,
        "deadDocFragmentBytes" : 98304000,
        "storageSegmentBase" : {
            "totalDocFragmentsCount" : 30000000,
            "deadDocFragmentsCount" : 1500000,
            "deadDocFragmentsPercent" : 5.0,
            "deadDocFragmentBytes" : 65536000
        },
        "storageSegmentExtended" : {
            "totalDocFragmentsCount" : 15000000,
            "deadDocFragmentsCount" : 750000,
            "deadDocFragmentsPercent" : 5.0,
            "deadDocFragmentBytes" : 32768000
        }
    },
    "collScans" : 14,
    "count" : 30000000,
    "size" : 1320000000,
    "avgObjSize" : 44,
    "storageSize" : 6461497344,
    "storageSizeStats" : {
        "storageSegmentBase" : 4307664896,
        "storageSegmentExtended" : 2153832448
    },
    "capped" : false,
    "nindexes" : 2,
    "totalIndexSize" : 9649553408,
    "indexSizes" : {
        "_id_" : 1910661120,
        "c_1" : 7738892288
    },
    "unusedStorageSize" : {
        "unusedBytes" : 4201881600,
        "unusedPercent" : 65.05,
        "storageSegmentBase" : {
            "unusedBytes" : 2801254400,
            "unusedPercent" : 65.05
        },
        "storageSegmentExtended" : {
            "unusedBytes" : 1400627200,
            "unusedPercent" : 65.05
        }
    },
```

```
    "cacheStats" : {
        "collBlksHit" : 171659016,
        "collBlksRead" : 754061,
        "collHitRatio" : 99.5627,
        "idxBlksHit" : 692563636,
        "idxBlksRead" : 1177921,
        "idxHitRatio" : 99.8303
    },
    "idxScans" : 41823984,
    "opCounter" : {
        "numDocsIns" : 0,
        "numDocsUpd" : 20911992,
        "numDocsDel" : 0
    },
    "lastReset" : "2025-06-24 05:57:08.219711+00",
    "ok" : 1,
    "operationTime" : Timestamp(1750968826, 1)
}
```

Preguntas frecuentes

¿Cómo puedo identificar si la recopilación de elementos no utilizados no funciona de manera eficiente?

Supervise estas señales de advertencia que indican una recopilación de elementos no utilizados ineficiente:

- Recolección excesiva: `unusedStorageSize` las métricas aumentan de forma constante durante las escrituras intensivas o las eliminaciones masivas, especialmente cuando se trata de índices de gran tamaño.
- Alto porcentaje de fragmentos muertos: `documentFragmentStats` muestra `deadDocFragmentsPercent` valores altos de forma constante (por encima del 10 al 15%).
- Latencia de consulta reducida: aumento de la latencia de consulta debido a la acumulación de documentos inactivos.
- Duración extendida del GC: las operaciones de recolección de basura tardan más que los promedios históricos. `gcRuntimeStats`
- Procesamiento de GC elevado: un nivel alto `LongestActiveGCRuntime` indica que el recolector de basura no puede satisfacer las demandas del sistema.

¿La recopilación de elementos no utilizados afecta al rendimiento de mi base de datos?

En condiciones normales, la recopilación de elementos no utilizados tiene un impacto mínimo en el rendimiento. Sin embargo, si la recopilación de elementos no utilizados se retrasa, puede experimentar lo siguiente:

- Aumento de los costes de almacenamiento debido a la acumulación de documentos muertos.
- El rendimiento de las consultas es más lento debido a las entradas de índice obsoletas.
- Modo temporal de solo lectura si los MVCC IDs están agotados.
- Mayor uso de recursos durante las ejecuciones de recopilación intensivas, especialmente en instancias más pequeñas.
- Reducción de la eficiencia en las operaciones del segmento de almacenamiento ampliado para documentos de gran tamaño.

¿Puedo activar manualmente la recopilación de elementos no utilizados?

No, la recopilación de elementos no utilizados en Amazon DocumentDB no se puede activar manualmente. El sistema administra la recopilación de elementos no utilizados automáticamente como parte de sus operaciones de mantenimiento interno.

¿Qué alarmas debo configurar como práctica operativa recomendada?

Recomendamos configurar la supervisión tanto a nivel de clúster como de colección para garantizar un rendimiento óptimo del sistema de Amazon DocumentDB.

Para la supervisión a nivel de clúster, comience por crear una CloudWatch alarma de Amazon para la `AvailableMVCCIds` métrica con un umbral de 1300 millones. Esto le da tiempo suficiente para tomar medidas antes de que la métrica llegue a cero, momento en el que el clúster pasará al modo de solo lectura. Ten en cuenta que esta métrica puede fluctuar en función de tus patrones de uso específicos: algunos clientes ven que cae por debajo de los 1 300 millones y luego se recupera por encima de los 1500 millones a medida que la recolección de basura termina su función.

También es importante monitorear la `LongestActiveGCRuntime` métrica a través de Amazon CloudWatch. Esta métrica, junto con `gcRuntimeStats`, le permite comprender el rendimiento de la recopilación de elementos no utilizados en todo el sistema.

Para el monitoreo a nivel de colección, concéntrate en estas métricas clave:

- `MVCCIdScale`— Esté atento al aumento de los valores que sugieren que los MVCC IDs están envejeciendo y que podrían necesitar atención.
- `gcRuntimeStats`— Identifique los procesos de recolección de basura que demoran inusualmente o se prolongan durante varios días.
- `documentFragmentStats`— Supervise `deadDocFragmentsPercent` los valores: los porcentajes altos y constantes (superiores al 10-15%) pueden indicar un retraso en la recogida de basura.
- `storageSizeStats`y `unusedStorageSize` — Realice un seguimiento de los patrones de uso del almacenamiento e identifique las colecciones con una cantidad significativa de espacio no utilizado en cualquiera de los segmentos de almacenamiento.

Las colecciones con operaciones de escritura frecuentes requieren atención especial, ya que generan más trabajo para el recopilador de elementos no utilizados. Le recomendamos que compruebe estas métricas con más frecuencia en las colecciones con mucha actividad de escritura para garantizar que la recopilación de elementos no utilizados esté a la altura de su carga de trabajo.

Tenga en cuenta que estas recomendaciones de supervisión sirven de punto de partida. A medida que se familiarice con el comportamiento de su sistema, tal vez desee ajustar estos umbrales para que se adapten mejor a sus patrones y requisitos de uso específicos.

¿Qué debo hacer si **`AvailableMVCCIds`** disminuye por debajo de los 1300 millones?

Si la métrica `AvailableMVCCIds` disminuye por debajo de los 1300 millones, le recomendamos que tome medidas inmediatas para evitar que el clúster entre en modo de solo lectura. Le recomendamos que primero amplíe el tamaño de la instancia para proporcionar más recursos informáticos al recopilador de elementos no utilizados. Esta es nuestra principal recomendación, ya que permite que su aplicación continúe con sus operaciones normales y, al mismo tiempo, le da al recolector de basura la potencia adicional que necesita para ponerse al día.

Si la ampliación por sí sola no mejora la situación, le recomendamos que considere reducir las operaciones de escritura. Utilice la `MVCCIdScale` métrica para identificar qué colecciones específicas contienen MVCC más antiguas y IDs que requieren atención. Además, supervise `documentFragmentStats` para identificar las colecciones con altos porcentajes de fragmentos muertos que puedan estar contribuyendo a la ineficiencia de la recolección de basura.

Una vez que haya identificado estas colecciones, es posible que tenga que reducir temporalmente las operaciones de escritura en ellas para permitir que la recopilación de elementos no utilizados se

ponga al día. Durante el período de recuperación, le recomendamos que supervise atentamente la métrica `AvailableMVCCIds` para asegurarse de que sus acciones tengan el efecto deseado. Se considera que el clúster está en buen estado una vez que el valor `AvailableMVCCIds` vuelve a ser 1500 millones o más.

Recuerde que estos pasos son medidas preventivas para ayudar a que su sistema se recupere antes de que alcance un estado crítico. Cuanto antes tome medidas tras ver la disminución de la métrica por debajo de los 1300 millones, más probabilidades tendrá de evitar que sus operaciones de escritura se vean afectadas.

Referencia de la API para la administración de recursos, instancias y clústeres de Amazon DocumentDB

En esta sección se describen las operaciones de administración de recursos, instancias y clústeres de Amazon DocumentDB (con compatibilidad con MongoDB) que se puede obtener acceso por medio de HTTP, la AWS Command Line Interface (AWS CLI) o el SDK de AWS. Puede utilizar estas API para crear, eliminar y modificar clústeres e instancias.

> **Important**
>
> Estas API solo se usan para la administración de clústeres, instancias y recursos relacionados. Para obtener información sobre cómo conectarse con un clúster de Amazon DocumentDB en ejecución, consulte Guía de introducción.

Temas

- Acciones
- Data Types
- Errores comunes
- Parámetros comunes

Acciones

admiten las siguientes acciones Amazon DocumentDB (with MongoDB compatibility):

- AddSourceIdentifierToSubscription
- AddTagsToResource
- ApplyPendingMaintenanceAction
- CopyDBClusterParameterGroup
- CopyDBClusterSnapshot
- CreateDBCluster
- CreateDBClusterParameterGroup
- CreateDBClusterSnapshot

- CreateDBInstance
- CreateDBSubnetGroup
- CreateEventSubscription
- CreateGlobalCluster
- DeleteDBCluster
- DeleteDBClusterParameterGroup
- DeleteDBClusterSnapshot
- DeleteDBInstance
- DeleteDBSubnetGroup
- DeleteEventSubscription
- DeleteGlobalCluster
- DescribeCertificates
- DescribeDBClusterParameterGroups
- DescribeDBClusterParameters
- DescribeDBClusters
- DescribeDBClusterSnapshotAttributes
- DescribeDBClusterSnapshots
- DescribeDBEngineVersions
- DescribeDBInstances
- DescribeDBSubnetGroups
- DescribeEngineDefaultClusterParameters
- DescribeEventCategories
- DescribeEvents
- DescribeEventSubscriptions
- DescribeGlobalClusters
- DescribeOrderableDBInstanceOptions
- DescribePendingMaintenanceActions
- FailoverDBCluster
- FailoverGlobalCluster
- ListTagsForResource

- ModifyDBCluster
- ModifyDBClusterParameterGroup
- ModifyDBClusterSnapshotAttribute
- ModifyDBInstance
- ModifyDBSubnetGroup
- ModifyEventSubscription
- ModifyGlobalCluster
- RebootDBInstance
- RemoveFromGlobalCluster
- RemoveSourceIdentifierFromSubscription
- RemoveTagsFromResource
- ResetDBClusterParameterGroup
- RestoreDBClusterFromSnapshot
- RestoreDBClusterToPointInTime
- StartDBCluster
- StopDBCluster
- SwitchoverGlobalCluster

Los clústeres elásticos de Amazon DocumentDB admiten las siguientes acciones:

- ApplyPendingMaintenanceAction
- CopyClusterSnapshot
- CreateCluster
- CreateClusterSnapshot
- DeleteCluster
- DeleteClusterSnapshot
- GetCluster
- GetClusterSnapshot
- GetPendingMaintenanceAction
- ListClusters
- ListClusterSnapshots

- ListPendingMaintenanceActions
- ListTagsForResource
- RestoreClusterFromSnapshot
- StartCluster
- StopCluster
- TagResource
- UntagResource
- UpdateCluster

Amazon DocumentDB (with MongoDB compatibility)

admiten las siguientes acciones Amazon DocumentDB (with MongoDB compatibility):

- AddSourceIdentifierToSubscription
- AddTagsToResource
- ApplyPendingMaintenanceAction
- CopyDBClusterParameterGroup
- CopyDBClusterSnapshot
- CreateDBCluster
- CreateDBClusterParameterGroup
- CreateDBClusterSnapshot
- CreateDBInstance
- CreateDBSubnetGroup
- CreateEventSubscription
- CreateGlobalCluster
- DeleteDBCluster
- DeleteDBClusterParameterGroup
- DeleteDBClusterSnapshot
- DeleteDBInstance
- DeleteDBSubnetGroup
- DeleteEventSubscription
- DeleteGlobalCluster

- DescribeCertificates
- DescribeDBClusterParameterGroups
- DescribeDBClusterParameters
- DescribeDBClusters
- DescribeDBClusterSnapshotAttributes
- DescribeDBClusterSnapshots
- DescribeDBEngineVersions
- DescribeDBInstances
- DescribeDBSubnetGroups
- DescribeEngineDefaultClusterParameters
- DescribeEventCategories
- DescribeEvents
- DescribeEventSubscriptions
- DescribeGlobalClusters
- DescribeOrderableDBInstanceOptions
- DescribePendingMaintenanceActions
- FailoverDBCluster
- FailoverGlobalCluster
- ListTagsForResource
- ModifyDBCluster
- ModifyDBClusterParameterGroup
- ModifyDBClusterSnapshotAttribute
- ModifyDBInstance
- ModifyDBSubnetGroup
- ModifyEventSubscription
- ModifyGlobalCluster
- RebootDBInstance
- RemoveFromGlobalCluster
- RemoveSourceIdentifierFromSubscription
- RemoveTagsFromResource

- ResetDBClusterParameterGroup
- RestoreDBClusterFromSnapshot
- RestoreDBClusterToPointInTime
- StartDBCluster
- StopDBCluster
- SwitchoverGlobalCluster

AddSourceIdentifierToSubscription

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Agrega un identificador de origen a una suscripción de notificación de eventos existente.

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

SourceIdentifier

El identificador del origen de eventos que se va a añadir:

- Si el tipo de origen es una instancia, debe proporcionarse un `DBInstanceIdentifier`.
- Si el tipo de origen es un grupo de seguridad, debe proporcionarse un `DBSecurityGroupName`.
- Si el tipo de origen es un grupo de parámetros, debe proporcionarse un `DBParameterGroupName`.
- Si el tipo de origen es una instantánea de base de datos, debe proporcionarse un `DBSnapshotIdentifier`.

Tipo: cadena

Obligatorio: sí

SubscriptionName

El nombre de la suscripción a notificaciones de eventos de Amazon DocumentDB al que desea añadir un identificador de origen.

Tipo: cadena

Obligatorio: sí

Elementos de respuesta

El servicio devuelve el siguiente elemento.

EventSubscription

Información detallada sobre un evento al que se ha suscrito.

Tipo: objeto EventSubscription

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

SourceNotFound

No se ha encontrado el origen solicitado.

Código de estado HTTP: 404

SubscriptionNotFound

El nombre de la suscripción no existe.

Código de estado HTTP: 404

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

AddTagsToResource

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Añade etiquetas de metadatos a un recurso de Amazon DocumentDB. Puede utilizar estas etiquetas con los informes de asignación de costos para realizar un seguimiento de los costos asociados a los recursos de Amazon DocumentDB o en una declaración de `Condition` de una política de AWS Identity and Access Management (IAM) para Amazon DocumentDB.

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

ResourceName

El recurso de Amazon DocumentDB al que se añaden las etiquetas. Este valor es un Nombre de recurso de Amazon (ARN).

Tipo: cadena

Obligatorio: sí

Tags.Tag.N

Las etiquetas que se van a asignar al recurso de Amazon DocumentDB.

Tipo: matriz de objetos Tag

Obligatorio: sí

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

DBClusterNotFoundFault

`DBClusterIdentifier` no hace referencia a un clúster existente.

Código de estado HTTP: 404

DBInstanceNotFound

`DBInstanceIdentifier` no hace referencia a una instancia existente.

Código de estado HTTP: 404

DBSnapshotNotFound

`DBSnapshotIdentifier` no hace referencia a una instantánea existente.

Código de estado HTTP: 404

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

ApplyPendingMaintenanceAction

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Aplica una acción de mantenimiento pendiente a un recurso (por ejemplo, a una instancia de Amazon DocumentDB).

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

ApplyAction

La acción de mantenimiento pendiente que se aplica a este recurso.

Valores válidos: `system-update`, `db-upgrade`

Tipo: cadena

Obligatorio: sí

OptInType

Un valor que especifica el tipo de solicitud de alta o deshace una solicitud de alta. Una solicitud de alta de tipo `immediate` no se puede deshacer.

Valores válidos:

- `immediate`: aplicar inmediatamente la acción de mantenimiento.
- `next-maintenance`: aplicar la acción de mantenimiento durante la siguiente ventana de mantenimiento del recurso.
- `undo-opt-in`: cancelar todas las solicitudes de alta `next-maintenance` existentes.

Tipo: cadena

Obligatorio: sí

ResourceIdentifier

El Nombre de recurso de Amazon (ARN) del recurso al que se aplica la acción de mantenimiento pendiente.

Tipo: cadena

Obligatorio: sí

Elementos de respuesta

El servicio devuelve el siguiente elemento.

ResourcePendingMaintenanceActions

Representa la salida de ApplyPendingMaintenanceAction.

Tipo: objeto ResourcePendingMaintenanceActions

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidDBClusterStateFault

El clúster no se encuentra en un estado válido.

Código de estado HTTP: 400

InvalidDBInstanceState

La instancia especificada no se encuentra en el estado disponible.

Código de estado HTTP: 400

ResourceNotFoundFault

No se ha encontrado el ID del recurso especificado.

Código de estado HTTP: 404

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET

- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

CopyDBClusterParameterGroup

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Copia el grupo de parámetros de clúster especificado.

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

SourceDBClusterParameterGroupIdentifier

El identificador o Nombre de recurso de Amazon (ARN) para el grupo de parámetros de clúster de origen.

Restricciones:

- Debe especificar un grupo de parámetros de clúster válido.
- Si el grupo de parámetros de clúster de origen es el mismo Región de AWS que el de la copia, especifique un identificador de grupo de parámetros válido; por ejemplo, `my-db-cluster-param-group`, o un ARN válido.
- Si el grupo de parámetros de origen está en un ARN distinto Región de AWS al de la copia, especifique un ARN de grupo de parámetros de clúster válido; por ejemplo, `arn:aws:rds:us-east-1:123456789012:sample-cluster:sample-parameter-group`.

Tipo: cadena

Obligatorio: sí

TargetDBClusterParameterGroupDescription

Descripción del grupo de parámetros de clúster copiado.

Tipo: cadena

Obligatorio: sí

TargetDBClusterParameterGroupIdentifier

El identificador para el grupo de parámetros de clúster copiado.

Restricciones:

- No puede ser nulo ni estar vacío o en blanco.
- Deben contener de 1 a 255 caracteres (letras, números o guiones).
- El primer carácter debe ser una letra.
- No puede terminar por un guion ni contener dos guiones consecutivos.

Ejemplo:: `my-cluster-param-group1`

Tipo: cadena

Obligatorio: sí

Tags.Tag.N

Las etiquetas que deben asignarse al grupo de parámetros.

Tipo: matriz de objetos Tag

Obligatorio: no

Elementos de respuesta

El servicio devuelve el siguiente elemento.

DBClusterParameterGroup

Información detallada sobre un grupo de parámetros de clúster.

Tipo: objeto DBClusterParameterGroup

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

DBParameterGroupAlreadyExists

Existe un grupo de parámetros con el mismo nombre.

Código de estado HTTP: 400

DBParameterGroupNotFound

`DBParameterGroupName` no hace referencia a un grupo de parámetros existente.

Código de estado HTTP: 404

DBParameterGroupQuotaExceeded

Esta solicitud provocaría que superara el número permitido de grupos de parámetros.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

CopyDBClusterSnapshot

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Copia una instantánea de un clúster.

Para copiar una instantánea del clúster de una instantánea manual del clúster compartida, `SourceDBClusterSnapshotIdentifier` debe ser el Nombre de recurso de Amazon (ARN) de la instantánea del clúster compartida. Solo puede copiar una instantánea de clúster de base de datos compartidos, cifrada o no, en la misma Región de AWS.

Para cancelar la operación de copia después de que esté en curso, elimine la instantánea de clúster de destino identificada por `TargetDBClusterSnapshotIdentifier` mientras esa instantánea de clúster está en estado de copia.

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

SourceDBClusterSnapshotIdentifier

El identificador de la instantánea del clúster que se va a copiar. Este parámetro no distingue entre mayúsculas y minúsculas.

Restricciones:

- Se debe especificar una instantánea del clúster válida cuyo estado sea disponible.
- Si la instantánea del clúster de origen está en la misma Región de AWS que la copia, especifique un identificador de instantánea válido.
- Si la instantánea del clúster de origen está en una cuenta de Región de AWS diferente o propiedad de otra cuenta de AWS, especifique el ARN de la instantánea.

Ejemplo:: `my-cluster-snapshot1`

Tipo: cadena

Obligatorio: sí

TargetDBClusterSnapshotIdentifier

El identificador de la nueva instantánea del clúster que se va a crear a partir de la instantánea del clúster de origen. Este parámetro no distingue entre mayúsculas y minúsculas.

Restricciones:

- Deben contener de 1 a 63 caracteres (letras, números o guiones).
- El primer carácter debe ser una letra.
- No puede terminar por un guion ni contener dos guiones consecutivos.

Ejemplo:: `my-cluster-snapshot2`

Tipo: cadena

Obligatorio: sí

CopyTags

Establezca a `true` para copiar todas las etiquetas de la instantánea del clúster de origen a la instantánea del clúster de destino, y en caso contrario `false`. El valor predeterminado es `false`.

Tipo: Booleano

Obligatorio: no

KmsKeyId

ID de la clave de AWS KMS de una instantánea del clúster de base de datos cifrada. El ID de clave de AWS KMS es el nombre de recurso de Amazon (ARN), el identificador de clave de AWS KMS o el alias de clave de AWS KMS de la clave de cifrado de AWS KMS.

Si copia una instantánea de clúster cifrada desde su Cuenta de AWS, puede especificar un valor `KmsKeyId` para cifrar la copia con una nueva clave de cifrado AWS KMS. Si no especifica ningún valor para `KmsKeyId`, la copia de la instantánea del clúster de base de datos se cifra con la misma clave de AWS KMS que la instantánea del clúster de origen.

Si copia una instantánea del clúster de base de datos cifrada que se ha compartido desde otra Cuenta de AWS, debe especificar un valor para `KmsKeyId`.

Para copiar una instantánea de un clúster cifrado en otra Región de AWS, establezca `KmsKeyId` en el identificador de la clave AWS KMS que va a usar para cifrar la copia de la instantánea de un clúster en la región de destino. Las claves de cifrado de AWS KMS son específicas para la Región de AWS en la que se han creado y no puede usar claves de cifrado de una Región de AWS en otra Región de AWS.

Si intenta copiar un snapshot de clúster de base de datos sin cifrar y especificar un valor para el parámetro `KmsKeyId`, se devuelve un error.

Tipo: cadena

Requerido: no

PreSignedUrl

La URL que contiene una solicitud firmada de Signature Version 4 para la operación `CopyDBClusterSnapshot` de la API en la Región de AWS que contiene la instantánea del clúster de origen que se desea copiar. Debe usar el parámetro `PreSignedUrl` al copiar una instantánea de un clúster de otra Región de AWS.

Si utiliza una herramienta del SDK de AWS o la AWS CLI, puede especificar la `SourceRegion` (o `--source-region` para la AWS CLI) en lugar de especificar `PreSignedUrl` manualmente. Especificando `SourceRegion` autogenerar una URL prefirmada que es una solicitud válida para la operación que se puede ejecutar en la fuente Región de AWS.

La URL prefirmada debe ser una solicitud válida para la operación de la API `CopyDBClusterSnapshot` que se pueda ejecutar en la Región de AWS de origen que contiene la instantánea del clúster que se va a copiar. La solicitud de la URL prefirmada debe contener los siguientes valores de parámetros:

- `SourceRegion`: el identificador de la región que contiene la instantánea que se va a copiar.
- `SourceDBClusterSnapshotIdentifier`: identificador de la instantánea del clúster cifrada que se va a copiar. Este identificador debe estar en el formato de Nombre de recurso de Amazon (ARN) para la de origen Región de AWS. Por ejemplo, si copia una instantánea de clúster cifrada de la región us-east-1 Región de AWS, el `SourceDBClusterSnapshotIdentifier` tendrá un aspecto similar al del siguiente ejemplo: `arn:aws:rds:us-east-1:12345678012:sample-cluster:sample-cluster-snapshot`.
- `TargetDBClusterSnapshotIdentifier`: identificador de la instantánea del clúster que se va a copiar. Este parámetro no distingue entre mayúsculas y minúsculas.

Tipo: cadena

Requerido: no

Tags.Tag.N

Las etiquetas que se van a asignar a la instantánea del clúster.

Tipo: matriz de objetos Tag

Obligatorio: no

Elementos de respuesta

El servicio devuelve el siguiente elemento.

DBClusterSnapshot

Información detallada sobre una instantánea de un clúster.

Tipo: objeto DBClusterSnapshot

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

DBClusterSnapshotAlreadyExistsFault

El usuario ya tiene una instantánea del clúster con el identificador concreto.

Código de estado HTTP: 400

DBClusterSnapshotNotFoundFault

`DBClusterSnapshotIdentifier` no hace referencia a una instantánea de un clúster existente.

Código de estado HTTP: 404

InvalidDBClusterSnapshotStateFault

El valor proporcionado no es un estado de instantánea de clúster válido.

Código de estado HTTP: 400

InvalidDBClusterStateFault

El clúster no se encuentra en un estado válido.

Código de estado HTTP: 400

KMSKeyNotAccessibleFault

Se ha producido un error al acceder a una clave de AWS KMS.

Código de estado HTTP: 400

SnapshotQuotaExceeded

La solicitud provocaría que superara el número de instantáneas permitido.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

CreateDBCluster

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Crea un nuevo clúster de Amazon DocumentDB.

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

DBClusterIdentifier

El identificador del clúster. Este parámetro se almacena como una cadena en minúsculas.

Restricciones:

- Deben contener de 1 a 63 caracteres (letras, números o guiones).
- El primer carácter debe ser una letra.
- No puede terminar por un guion ni contener dos guiones consecutivos.

Ejemplo:: `my-cluster`

Tipo: cadena

Obligatorio: sí

Engine

El nombre del motor de base de datos que se debe utilizar para este clúster.

Valores válidos: -.: `docdb`

Tipo: cadena

Obligatorio: sí

AvailabilityZones.AvailabilityZone.N

Una lista de zonas de disponibilidad de Amazon EC2 en las que se pueden crear instancias en el clúster.

Tipo: matriz de cadenas

Obligatorio: no

BackupRetentionPeriod

El número de días durante los que se retienen las copias de seguridad automatizadas. Debe especificar un valor mínimo de 1.

Valor predeterminado: 1

Restricciones:

- Debe ser un valor entre 1 y 35.

Tipo: entero

Obligatorio: no

DBClusterParameterGroupName

El nombre del grupo de parámetros del clúster para asociar a este clúster.

Tipo: cadena

Requerido: no

DBSubnetGroupName

Un grupo de subred con el que asociar este clúster.

Limitaciones: debe coincidir con el nombre de un existente `DBSubnetGroup`. No debe ser predeterminado.

Ejemplo:: `mySubnetgroup`

Tipo: cadena

Requerido: no

DeletionProtection

Especifica si se puede eliminar este clúster. Si `DeletionProtection` está habilitado, no se puede eliminar el clúster a menos que se modifique y `DeletionProtection` esté deshabilitado. `DeletionProtection` protege los clústeres de una eliminación accidental.

Tipo: Booleano

Obligatorio: no

EnableCloudwatchLogsExports.member.N

La lista de tipos de registro que deben habilitarse para exportar a Registros de Amazon CloudWatch. Puede habilitar los registros de auditoría o los registros del generador de perfiles. Para obtener más información, consulte Auditoría de eventos de Amazon DocumentDB y Creación de perfiles de operaciones de Amazon DocumentDB.

Tipo: matriz de cadenas

Obligatorio: no

EngineVersion

El número de versión del motor de base de datos que se debe usar. `--engine-version` será el valor predeterminado de la última versión principal del motor. Para las cargas de trabajo de producción, se recomienda declarar explícitamente este parámetro con la versión del motor principal prevista.

Tipo: cadena

Requerido: no

GlobalClusterIdentifier

Identificador de clúster del nuevo clúster global.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 255 caracteres.

Patrón: `[A-Za-z][0-9A-Za-z-:._]*`

Obligatorio: no

KmsKeyId

El identificador de la clave de AWS KMS de un clúster cifrado.

El identificador de la clave de AWS KMS es el nombre de recurso de Amazon (ARN) de la clave de cifrado de AWS KMS. Si está creando un clúster con la misma cuenta de la Cuenta de AWS a la que pertenece la clave de cifrado de AWS KMS utilizada para cifrar el clúster nuevo, puede utilizar el alias de la clave de AWS KMS en lugar del ARN para la clave de cifrado de AWS KMS.

Si no se especifica una clave de cifrado en `KmsKeyId`:

- Si el parámetro `StorageEncrypted` es `true`, Amazon DocumentDB utiliza la clave de cifrado predeterminada.

AWS KMS crea la clave de cifrado predeterminada para su Cuenta de AWS. Cada Cuenta de AWS dispone de una clave de cifrado predeterminada diferente para cada Regiones de AWS.

Tipo: cadena

Requerido: no

ManageMasterUserPassword

Especifica si se debe administrar la contraseña del usuario maestro con Secrets Manager de Amazon Web Services.

Restricción: No puede administrar la contraseña del usuario maestro con Secrets Manager de Amazon Web Services si la `MasterUserPassword` está especificada.

Tipo: Booleano

Obligatorio: no

MasterUsername

Nombre del usuario maestro del clúster.

Restricciones:

- Debe tener de 1 a 63 letras o números.
- El primer carácter debe ser una letra.
- No puede ser una palabra reservada para el motor de base de datos elegido.

Tipo: cadena

Requerido: no

MasterUserPassword

La contraseña del usuario de la base de datos maestra. Esta contraseña puede contener cualquier carácter ASCII imprimible, excepto barra inclinada (/), comillas dobles (") o el símbolo de “arroba” (@).

Limitaciones: debe contener de 8 a 100 caracteres.

Tipo: cadena

Requerido: no

MasterUserSecretKmsKeyId

El identificador de clave KMS de Amazon Web Services para cifrar un secreto que se genera y administra automáticamente en Secrets Manager de Amazon Web Services. Esta configuración solo es válida si Amazon DocumentDB administra la contraseña del usuario maestro en Secrets Manager de Amazon Web Services para el clúster de base de datos.

El identificador de la clave de KMS de Amazon Web Services es el ARN de la clave, el identificador de clave, el ARN de alias o el nombre de alias de la clave de KMS. Para utilizar una clave de KMS en una cuenta de Amazon Web Services diferente, debe especificar el ARN de la clave o el ARN del alias.

Si no especifica el `MasterUserSecretKmsKeyId`, se utiliza la clave de KMS de `aws/secretsmanager` para cifrar el secreto. Si el secreto está en una cuenta de Amazon Web Services diferente, entonces no puede usar la clave de KMS de `aws/secretsmanager` para cifrar el secreto y se debe usar una clave de KMS administrada por el cliente.

Existe una clave KMS predeterminada para su cuenta de Amazon Web Services. La cuenta de Amazon Web Services tiene una clave de KMS predeterminada diferente para cada región de Amazon Web Services.

Tipo: cadena

Requerido: no

NetworkType

El tipo de red del clúster.

El tipo de red viene determinado por el `DBSubnetGroup` especificado para el clúster. Un `DBSubnetGroup` admite solamente el protocolo IPv4 o los protocolos IPv4 e IPv6 (`DUAL`).

Para obtener más información, consulte Clústeres de DocumentDB en una VPC en la Guía para desarrolladores de Amazon DocumentDB.

Valores válidos: `IPV4` | `DUAL`

Tipo: cadena

Requerido: no

Port

El número de puerto en el que las instancias en el clúster aceptan conexiones.

Tipo: entero

Obligatorio: no

PreferredBackupWindow

El intervalo de tiempo diario durante el que se crean las copias de seguridad automatizadas si las copias de seguridad automatizadas están habilitadas con el parámetro `BackupRetentionPeriod`.

El valor predeterminado es una ventana de 30 minutos seleccionada al azar dentro de un bloque de 8 horas para cada Región de AWS.

Restricciones:

- Tiene que tener el formato `hh24:mi-hh24:mi`.
- Debe indicarse en Tiempo universal coordinado (UTC).
- No debe entrar en conflicto con la ventana de mantenimiento preferida.
- Debe durar al menos 30 minutos.

Tipo: cadena

Requerido: no

PreferredMaintenanceWindow

El intervalo de tiempo semanal durante el cual puede llevarse a cabo el mantenimiento del sistema, en tiempo universal coordinado (UTC).

Formato: `ddd:hh24:mi-ddd:hh24:mi`

El valor predeterminado es un periodo de 30 minutos seleccionado al azar de un bloque de 8 horas de tiempo para cada Región de AWS, que tiene lugar un día de la semana al azar.

Días válidos: lunes, martes, miércoles, jueves, viernes, sábado, domingo

Restricciones: ventana mínima de 30 minutos.

Tipo: cadena

Requerido: no

PreSignedUrl

No se admite actualmente.

Tipo: cadena

Requerido: no

ServerlessV2ScalingConfiguration

Contiene la configuración de escalado de un clúster de Amazon DocumentDB sin servidor.

Tipo: objeto ServerlessV2ScalingConfiguration

Obligatorio: no

StorageEncrypted

Especifica si el clúster está cifrado.

Tipo: Booleano

Obligatorio: no

StorageType

El tipo de almacenamiento que se va a asociar al clúster de base de datos.

Para obtener información sobre los tipos de almacenamiento de los clústeres de Amazon DocumentDB, consulte Cluster storage configurations en la Guía para desarrolladores de Amazon DocumentDB.

Valores válidos para el tipo de almacenamiento: `standard | iopt1`

El valor predeterminado es `standard`

> **Note**
>
> Si crea un clúster de Amazon DocumentDB con el tipo de almacenamiento establecido en `iopt1`, el tipo de almacenamiento aparece en la respuesta. El tipo de almacenamiento no se devuelve cuando se establece en `standard`.

Tipo: cadena

Requerido: no

Tags.Tag.N

Las etiquetas que se van a asignar al clúster.

Tipo: matriz de objetos Tag

Obligatorio: no

VpcSecurityGroupIds.VpcSecurityGroupId.N

Una lista de grupos de seguridad de VPC de EC2 para asociar a este clúster.

Tipo: matriz de cadenas

Obligatorio: no

Elementos de respuesta

El servicio devuelve el siguiente elemento.

DBCluster

Información detallada sobre un clúster.

Tipo: objeto DBCluster

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

DBClusterAlreadyExistsFault

El usuario ya tiene un clúster con el identificador concreto.

Código de estado HTTP: 400

DBClusterNotFoundFault

`DBClusterIdentifier` no hace referencia a un clúster existente.

Código de estado HTTP: 404

DBClusterParameterGroupNotFound

`DBClusterParameterGroupName` no hace referencia a un grupo de parámetros de clúster existente.

Código de estado HTTP: 404

DBClusterQuotaExceededFault

No se puede crear el clúster porque ha alcanzado la cuota de clústeres máxima permitida.

Código de estado HTTP: 403

DBInstanceNotFound

`DBInstanceIdentifier` no hace referencia a una instancia existente.

Código de estado HTTP: 404

DBSubnetGroupDoesNotCoverEnoughAZs

Las subredes del grupo de subredes deben incluir al menos dos zonas de disponibilidad a menos que solo haya una zona de disponibilidad.

Código de estado HTTP: 400

DBSubnetGroupNotFoundFault

`DBSubnetGroupName` no hace referencia a un grupo de subredes existente.

Código de estado HTTP: 404

GlobalClusterNotFoundFault

`GlobalClusterIdentifier` no hace referencia a un clúster global existente.

Código de estado HTTP: 404

InsufficientStorageClusterCapacity

No hay bastante almacenamiento disponible para la acción en curso. Es posible que pueda resolver este error mediante la actualización de su grupo de subredes para utilizar diferentes zonas de disponibilidad que tienen más almacenamiento disponible.

Código de estado HTTP: 400

InvalidDBClusterStateFault

El clúster no se encuentra en un estado válido.

Código de estado HTTP: 400

InvalidDBInstanceState

La instancia especificada no se encuentra en el estado disponible.

Código de estado HTTP: 400

InvalidDBSubnetGroupStateFault

El grupo de subredes no se puede eliminar porque está en uso.

Código de estado HTTP: 400

InvalidGlobalClusterStateFault

La operación solicitada no se puede realizar mientras el clúster esté en este estado.

Código de estado HTTP: 400

InvalidSubnet

La subred solicitada no es válida o se solicitaron varias subredes que no están en la misma nube privada virtual (VPC).

Código de estado HTTP: 400

InvalidVPCNetworkStateFault

El grupo de subredes no cubre todas las zonas de disponibilidad después de crearla, debido a los cambios realizados.

Código de estado HTTP: 400

KMSKeyNotAccessibleFault

Se ha producido un error al acceder a una clave de AWS KMS.

Código de estado HTTP: 400

NetworkTypeNotSupported

El tipo de red no es compatible con `DBSubnetGroup` ni con la versión del motor de base de datos.

Código de estado HTTP: 400

StorageQuotaExceeded

La solicitud provocaría que superara la cantidad permitida de almacenamiento disponible en todas las instancias.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

CreateDBClusterParameterGroup

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Crear un nuevo grupo de parámetros de clúster.

Los parámetros de un grupo de parámetros de clúster se aplican a todas las instancias de un clúster.

Un grupo de parámetros de clúster se crea inicialmente con los parámetros predeterminados para el motor de base de datos utilizado por las instancias del clúster. En Amazon DocumentDB, no puede realizar modificaciones directamente en el grupo de parámetros de clúster `default.docdb3.6`. Si el clúster de Amazon DocumentDB utiliza el grupo de parámetros de clúster predeterminado y desea modificar un valor en él, primero debe crear un nuevo grupo de parámetros o copiar un grupo de parámetros existente, modificarlo y, a continuación, aplicar el grupo de parámetros modificado a su clúster. Para que el nuevo grupo de parámetros de clúster y la configuración asociada surta efecto, debe reiniciar las instancias del clúster sin conmutación por error. Para obtener más información, consulte Modificación de grupos de parámetros de clúster de Amazon DocumentDB.

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

DBClusterParameterGroupName

El nombre del grupo de parámetros de clúster.

Restricciones:

- No debe coincidir con el nombre de un existente `DBClusterParameterGroup`.

> **Note**
>
> Este valor se almacena como una cadena en minúsculas.

Tipo: cadena

Obligatorio: sí

DBParameterGroupFamily

El nombre de la familia del grupo de parámetros de clúster.

Tipo: cadena

Obligatorio: sí

Description

Descripción del grupo de parámetros de clúster.

Tipo: cadena

Obligatorio: sí

Tags.Tag.N

Las etiquetas que se van a asignar al grupo de parámetros de clúster.

Tipo: matriz de objetos Tag

Obligatorio: no

Elementos de respuesta

El servicio devuelve el siguiente elemento.

DBClusterParameterGroup

Información detallada sobre un grupo de parámetros de clúster.

Tipo: objeto DBClusterParameterGroup

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

DBParameterGroupAlreadyExists

Existe un grupo de parámetros con el mismo nombre.

Código de estado HTTP: 400

DBParameterGroupQuotaExceeded

Esta solicitud provocaría que superara el número permitido de grupos de parámetros.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

CreateDBClusterSnapshot

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Crea una instantánea de un clúster.

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

DBClusterIdentifier

El identificador del clúster para el que se va a crear una instantánea. Este parámetro no distingue entre mayúsculas y minúsculas.

Restricciones:

- Debe coincidir con el identificador de un `DBCluster` existente.

Ejemplo:: `my-cluster`

Tipo: cadena

Obligatorio: sí

DBClusterSnapshotIdentifier

El identificador de la instantánea del clúster. Este parámetro se almacena como una cadena en minúsculas.

Restricciones:

- Deben contener de 1 a 63 caracteres (letras, números o guiones).
- El primer carácter debe ser una letra.
- No puede terminar por un guion ni contener dos guiones consecutivos.

Ejemplo:: `my-cluster-snapshot1`

Tipo: cadena

Obligatorio: sí

Tags.Tag.N

Las etiquetas que se van a asignar a la instantánea del clúster.

Tipo: matriz de objetos Tag

Obligatorio: no

Elementos de respuesta

El servicio devuelve el siguiente elemento.

DBClusterSnapshot

Información detallada sobre una instantánea de un clúster.

Tipo: objeto DBClusterSnapshot

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

DBClusterNotFoundFault

`DBClusterIdentifier` no hace referencia a un clúster existente.

Código de estado HTTP: 404

DBClusterSnapshotAlreadyExistsFault

El usuario ya tiene una instantánea del clúster con el identificador concreto.

Código de estado HTTP: 400

InvalidDBClusterSnapshotStateFault

El valor proporcionado no es un estado de instantánea de clúster válido.

Código de estado HTTP: 400

InvalidDBClusterStateFault

El clúster no se encuentra en un estado válido.

Código de estado HTTP: 400

SnapshotQuotaExceeded

La solicitud provocaría que superara el número de instantáneas permitido.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

CreateDBInstance

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Crea una nueva instancia.

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

DBClusterIdentifier

El identificador del clúster al que pertenecerá la instancia.

Tipo: cadena

Obligatorio: sí

DBInstanceClass

La capacidad de memoria e informática de la instancia (por ejemplo,)., `db.r5.large`.

Tipo: cadena

Obligatorio: sí

DBInstanceIdentifier

El identificador de instancias. Este parámetro se almacena como una cadena en minúsculas.

Restricciones:

- Deben contener de 1 a 63 caracteres (letras, números o guiones).
- El primer carácter debe ser una letra.
- No puede terminar por un guion ni contener dos guiones consecutivos.

Ejemplo:: `mydbinstance`

Tipo: cadena

Obligatorio: sí

Engine

Nombre del motor de base de datos que se va a usar para esta instancia.

Valor válido: `docdb`

Tipo: cadena

Obligatorio: sí

AutoMinorVersionUpgrade

Este parámetro no se aplica a Amazon DocumentDB. Amazon DocumentDB no actualiza versiones secundarias, independientemente del valor establecido.

Predeterminado: `false`

Tipo: Booleano

Obligatorio: no

AvailabilityZone

La zona de disponibilidad de Amazon EC2 en la que se crea la instancia.

Predeterminado: una zona de disponibilidad aleatoria elegida por el sistema en la Región de AWS del punto de conexión.

Ejemplo:: `us-east-1d`

Tipo: cadena

Requerido: no

CACertificateIdentifier

El identificador del certificado de CA que se utilizará para el certificado de servidor de la instancia de DB.

Para obtener más información, consulte Cómo actualizar los certificados TLS de Amazon DocumentDB y Cómo cifrar datos en tránsito en la Guía para desarrolladores de Amazon DocumentDB.

Tipo: cadena

Requerido: no

CopyTagsToSnapshot

Es un valor que indica si se deben copiar las etiquetas de la instancia de base de datos en instantáneas de la instancia de base de datos. Las etiquetas no se copian de forma predeterminada.

Tipo: Booleano

Obligatorio: no

EnablePerformanceInsights

Un valor que indica si se habilita Información sobre rendimiento para la instancia de base de datos. Para obtener más información, consulte Uso de Información sobre rendimiento de Amazon.

Tipo: Booleano

Obligatorio: no

PerformanceInsightsKMSKeyId

El identificador de la clave de AWS KMS para el cifrado de datos de Performance Insights.

El identificador de la clave de AWS KMS es el ARN de la clave, el identificador de clave, el ARN de alias o el nombre de alias de la clave de KMS.

Si no especifica un valor para PerformanceInsightsKMSKeyId, Amazon DocumentDB utilizará su clave KMS predeterminada. Existe una clave KMS predeterminada para su cuenta de Amazon Web Services. La cuenta de Amazon Web Services tiene una clave de KMS predeterminada diferente para cada región de Amazon Web Services.

Tipo: cadena

Requerido: no

PreferredMaintenanceWindow

El intervalo de tiempo semanal durante el cual puede llevarse a cabo el mantenimiento del sistema, en tiempo universal coordinado (UTC).

Formato: `ddd:hh24:mi-ddd:hh24:mi`

El valor predeterminado es un periodo de 30 minutos seleccionado al azar de un bloque de 8 horas de tiempo para cada Región de AWS, que tiene lugar un día de la semana al azar.

Días válidos: lunes, martes, miércoles, jueves, viernes, sábado, domingo

Restricciones: ventana mínima de 30 minutos.

Tipo: cadena

Requerido: no

PromotionTier

Valor que especifica el orden en el que se promueve una réplica de Amazon DocumentDB a la instancia primaria tras un fallo de la instancia primaria existente.

Valor predeterminado: 1

Valores válidos: 0-15

Tipo: entero

Obligatorio: no

Tags.Tag.N

Las etiquetas que se van a asignar a la instancia. Puede asignar hasta 10 etiquetas a una instancia.

Tipo: matriz de objetos Tag

Obligatorio: no

Elementos de respuesta

El servicio devuelve el siguiente elemento.

DBInstance

Información detallada sobre una instancia.

Tipo: objeto DBInstance

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

AuthorizationNotFound

La IP CIDR o el grupo de seguridad de Amazon EC2 especificados no están autorizados para el grupo de seguridad especificado.

Es posible que Amazon DocumentDB tampoco esté autorizado para realizar las acciones necesarias en su nombre mediante IAM.

Código de estado HTTP: 404

DBClusterNotFoundFault

`DBClusterIdentifier` no hace referencia a un clúster existente.

Código de estado HTTP: 404

DBInstanceAlreadyExists

Ya tiene una instancia con el identificador dado.

Código de estado HTTP: 400

DBParameterGroupNotFound

`DBParameterGroupName` no hace referencia a un grupo de parámetros existente.

Código de estado HTTP: 404

DBSecurityGroupNotFound

`DBSecurityGroupName` no hace referencia a un grupo de seguridad existente.

Código de estado HTTP: 404

DBSubnetGroupDoesNotCoverEnoughAZs

Las subredes del grupo de subredes deben incluir al menos dos zonas de disponibilidad a menos que solo haya una zona de disponibilidad.

Código de estado HTTP: 400

DBSubnetGroupNotFoundFault

`DBSubnetGroupName` no hace referencia a un grupo de subredes existente.

Código de estado HTTP: 404

InstanceQuotaExceeded

La solicitud provocaría que se superara el número de instancias permitido.

Código de estado HTTP: 400

InsufficientDBInstanceCapacity

La clase de instancia especificada no está disponible en la zona de disponibilidad especificada.

Código de estado HTTP: 400

InvalidDBClusterStateFault

El clúster no se encuentra en un estado válido.

Código de estado HTTP: 400

InvalidSubnet

La subred solicitada no es válida o se solicitaron varias subredes que no están en la misma nube privada virtual (VPC).

Código de estado HTTP: 400

InvalidVPCNetworkStateFault

El grupo de subredes no cubre todas las zonas de disponibilidad después de crearla, debido a los cambios realizados.

Código de estado HTTP: 400

KMSKeyNotAccessibleFault

Se ha producido un error al acceder a una clave de AWS KMS.

Código de estado HTTP: 400

StorageQuotaExceeded

La solicitud provocaría que superara la cantidad permitida de almacenamiento disponible en todas las instancias.

Código de estado HTTP: 400

StorageTypeNotSupported

El almacenamiento del `StorageType` especificado no puede asociarse a la instancia de base de datos.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

CreateDBSubnetGroup

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Crea un nuevo grupo de subredes. Los grupos de subredes deben contener al menos una subred en al menos dos zonas de disponibilidad de la Región de AWS.

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

DBSubnetGroupDescription

La descripción del grupo de subredes.

Tipo: cadena

Obligatorio: sí

DBSubnetGroupName

El nombre del grupo de subredes. Este valor se almacena como una cadena en minúsculas.

Restricciones: debe contener un máximo de 255 letras, números, puntos, guiones bajos, espacios o guiones. No debe ser predeterminado.

Ejemplo:: `mySubnetgroup`

Tipo: cadena

Obligatorio: sí

SubnetIds.SubnetIdentifier.N

Los ID de subred de Amazon EC2 para el grupo de subredes.

Tipo: matriz de cadenas

Obligatorio: sí

Tags.Tag.N

La etiqueta que se va a asignar al grupo de subredes.

Tipo: matriz de objetos Tag

Obligatorio: no

Elementos de respuesta

El servicio devuelve el siguiente elemento.

DBSubnetGroup

Información detallada sobre un grupo de subredes.

Tipo: objeto DBSubnetGroup

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

DBSubnetGroupAlreadyExists

Un grupo de subredes existente ya está utilizando `DBSubnetGroupName`.

Código de estado HTTP: 400

DBSubnetGroupDoesNotCoverEnoughAZs

Las subredes del grupo de subredes deben incluir al menos dos zonas de disponibilidad a menos que solo haya una zona de disponibilidad.

Código de estado HTTP: 400

DBSubnetGroupQuotaExceeded

La solicitud provocaría que se superara el número de grupos de subredes permitidos.

Código de estado HTTP: 400

DBSubnetQuotaExceededFault

La solicitud le haría exceder el número permitido de subredes en un grupo de subredes.

Código de estado HTTP: 400

InvalidSubnet

La subred solicitada no es válida o se solicitaron varias subredes que no están en la misma nube privada virtual (VPC).

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- SDK de AWS para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK de para Ruby V3

CreateEventSubscription

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Crea una suscripción de notificación de eventos de Amazon DocumentDB. Esta acción requiere un nombre de recurso de Amazon (ARN) de tema creado por la consola de Amazon DocumentDB, la consola de Amazon SNS o la API de Amazon SNS. Para obtener un ARN con Amazon SNS, debe crear un tema en Amazon SNS y suscribirse al tema. El ARN se muestra en la consola de Amazon SNS.

Puede especificar el tipo de origen (`SourceType`) sobre el que desea recibir notificaciones. También puede proporcionar una lista de las fuentes de Amazon DocumentDB (`SourceIds`) que desencadenan los eventos y puede proporcionar una lista de categorías de eventos (`EventCategories`) para los eventos de los que desee recibir notificaciones. Por ejemplo, puede especificar `SourceType = db-instance`, `SourceIds = mydbinstance1, mydbinstance2` y `EventCategories = Availability, Backup`.

Si especifica ambos valores `SourceType` y `SourceIds`, como, por ejemplo, `SourceType = db-instance` y `SourceIdentifier = myDBInstance1`, recibirá todos los eventos `db-instance` del origen especificado. Si especifica un `SourceType`, pero no especifica `SourceIdentifier`, recibirá notificaciones de los eventos de ese tipo de origen para todos sus orígenes de Amazon DocumentDB. Si no especifica ni `SourceType` ni `SourceIdentifier`, recibirá notificaciones de los eventos generados desde todos los orígenes de Amazon DocumentDB que pertenezcan a su cuenta de cliente.

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

SnsTopicArn

El Nombre de recurso de Amazon (ARN) del tema SNS creado para la notificación de eventos. El ARN es creado por Amazon SNS al crear un tema y suscribirse a él.

Tipo: cadena

Obligatorio: sí

SubscriptionName

El nombre de la suscripción.

Restricciones: el nombre debe tener menos de 255 caracteres.

Tipo: cadena

Obligatorio: sí

Enabled

Establezca un valor booleano en `true` para activar la suscripción y en `false` para crear la suscripción, pero sin activarla.

Tipo: Booleano

Obligatorio: no

EventCategories.EventCategory.N

Una lista de las categorías de eventos para un `SourceType` a los que desea suscribirse.

Tipo: matriz de cadenas

Obligatorio: no

SourceIDS.SourceID.N

La lista de identificadores de los orígenes de eventos para los que se devuelven eventos. Si no se especifica, se incluyen todos los orígenes en la respuesta. Un identificador debe comenzar por una letra y solo deben contener letras ASCII, números y guiones; y no pueden terminar con un guion o contener dos guiones consecutivos.

Restricciones:

- Si se proporciona `SourceIds`, también se debe proporcionar `SourceType`.
- Si el tipo de origen es una instancia, debe proporcionarse un `DBInstanceIdentifier`.
- Si el tipo de origen es un grupo de seguridad, debe proporcionarse un `DBSecurityGroupName`.
- Si el tipo de origen es un grupo de parámetros, debe proporcionarse un `DBParameterGroupName`.
- Si el tipo de origen es una instantánea de base de datos, debe proporcionarse un `DBSnapshotIdentifier`.

Tipo: matriz de cadenas

Obligatorio: no

SourceType

El tipo de origen que está generando los eventos. Por ejemplo, si desea recibir una notificación de eventos generados por una instancia, defina este parámetro como `db-instance`. Si no se especifica este valor, se devuelven todos los eventos.

Valores válidos: `db-instance`, `db-cluster`, `db-parameter-group`, `db-security-group`, `db-cluster-snapshot`

Tipo: cadena

Requerido: no

Tags.Tag.N

Las etiquetas que se asignarán a la suscripción de eventos.

Tipo: matriz de objetos Tag

Obligatorio: no

Elementos de respuesta

El servicio devuelve el siguiente elemento.

EventSubscription

Información detallada sobre un evento al que se ha suscrito.

Tipo: objeto EventSubscription

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

EventSubscriptionQuotaExceeded

Ha alcanzado el número máximo de suscripciones a eventos.

Código de estado HTTP: 400

SNSInvalidTopic

Amazon SNS ha respondido que hay un problema con el tema especificado.

Código de estado HTTP: 400

SNSNoAuthorization

No tiene permiso para publicar en el tema SNS Nombre de recurso de Amazon (ARN).

Código de estado HTTP: 400

SNSTopicArnNotFound

El nombre de recurso de Amazon (ARN) del tema de SNS no existe.

Código de estado HTTP: 404

SourceNotFound

No se ha encontrado el origen solicitado.

Código de estado HTTP: 404

SubscriptionAlreadyExist

El nombre de suscripción proporcionado ya existe.

Código de estado HTTP: 400

SubscriptionCategoryNotFound

La categoría proporcionada no existe.

Código de estado HTTP: 404

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2

- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

CreateGlobalCluster

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Crea un clúster global de Amazon DocumentDB que puede abarcar varios múltiplos Regiones de AWS. El clúster global contiene un clúster principal con capacidad de lectura y escritura, y hasta 10 clústeres secundarios de solo lectura. Los clústeres globales utilizan una replicación rápida basada en el almacenamiento en todas las regiones con latencias inferiores a un segundo, mediante una infraestructura especializada que no afecta el rendimiento de la carga de trabajo.

Puede crear un clúster que inicialmente esté vacío y, a posteriormente agregarle un clúster principal y un clúster secundario. O bien, puede especificar un clúster existente durante la operación de creación y este clúster pasará a ser el principal del clúster global.

> **Note**
>
> Esta acción solo se aplica a los clústeres de Amazon DocumentDB.

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

GlobalClusterIdentifier

Identificador de clúster del nuevo clúster global.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 255 caracteres.

Patrón: `[A-Za-z][0-9A-Za-z-:._]*`

Obligatorio: sí

DatabaseName

El nombre para la base de datos de hasta 64 caracteres alfanuméricos. Si no proporciona un nombre, Amazon DocumentDB no creará una base de datos en el clúster global que está creando.

Tipo: cadena

Requerido: no

DeletionProtection

La configuración de protección contra eliminación para el nuevo clúster global. El clúster global no se puede eliminar cuando está habilitada la protección contra eliminación.

Tipo: Booleano

Obligatorio: no

Engine

El nombre del motor de base de datos que se debe utilizar para este clúster.

Tipo: cadena

Requerido: no

EngineVersion

La versión del motor del clúster global.

Tipo: cadena

Requerido: no

SourceDBClusterIdentifier

El i Nombre de recurso de Amazon (ARN) que se utilizará como clúster principal de la base de datos global. Este parámetro es opcional.

Tipo: cadena

Requerido: no

StorageEncrypted

Configuración de cifrado de almacenamiento para el nuevo clúster global.

Tipo: Booleano

Obligatorio: no

Elementos de respuesta

El servicio devuelve el siguiente elemento.

GlobalCluster

Tipo de datos que representa un clúster global de Amazon DocumentDB.

Tipo: objeto GlobalCluster

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

DBClusterNotFoundFault

`DBClusterIdentifier` no hace referencia a un clúster existente.

Código de estado HTTP: 404

GlobalClusterAlreadyExistsFault

El `GlobalClusterIdentifier` ya existe. Elija un nuevo identificador de clúster global (nombre único) para crear un nuevo clúster global.

Código de estado HTTP: 400

GlobalClusterQuotaExceededFault

El número de clústeres globales de esta cuenta ya es el máximo permitido.

Código de estado HTTP: 400

InvalidDBClusterStateFault

El clúster no se encuentra en un estado válido.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

DeleteDBCluster

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Elimina un clúster de aprovisionado anteriormente. Al eliminar un clúster, se eliminan todas las copias de seguridad automatizadas para ese clúster y no se pueden recuperar. Las instantáneas manuales del clúster de base de datos del clúster especificado no se eliminan.

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

DBClusterIdentifier

El identificador del clúster del clúster que se va a eliminar. Este parámetro no distingue entre mayúsculas y minúsculas.

Restricciones:

- Debe coincidir con un `DBClusterIdentifier` existente.

Tipo: cadena

Obligatorio: sí

FinalDBSnapshotIdentifier

El identificador de instantánea de clúster de la nueva instantánea del clúster creada al configurar `SkipFinalSnapshot` como `false`.

> **Note**
>
> Se especifica este parámetro y también el parámetro `SkipFinalShapshot` en `true` genera un error.

Restricciones:

- Debe tener de 1 a 255 letras, números o guiones.
- El primer carácter debe ser una letra.
- No puede terminar por un guion ni contener dos guiones consecutivos.

Tipo: cadena

Requerido: no

SkipFinalSnapshot

Determina si se crea una instantánea de clúster final antes de que se elimine el clúster. Si se especifica `true`, no se crea ninguna instantánea del clúster. Si se especifica `false`, se crea una instantánea de clúster antes de que se elimine el clúster de base de datos.

> **Note**
>
> Debe especificar un parámetro `FinalDBSnapshotIdentifier` si `SkipFinalSnapshot` es `false`.

Predeterminado: `false`

Tipo: Booleano

Obligatorio: no

Elementos de respuesta

El servicio devuelve el siguiente elemento.

DBCluster

Información detallada sobre un clúster.

Tipo: objeto DBCluster

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

DBClusterNotFoundFault

`DBClusterIdentifier` no hace referencia a un clúster existente.

Código de estado HTTP: 404

DBClusterSnapshotAlreadyExistsFault

El usuario ya tiene una instantánea del clúster con el identificador concreto.

Código de estado HTTP: 400

InvalidDBClusterSnapshotStateFault

El valor proporcionado no es un estado de instantánea de clúster válido.

Código de estado HTTP: 400

InvalidDBClusterStateFault

El clúster no se encuentra en un estado válido.

Código de estado HTTP: 400

SnapshotQuotaExceeded

La solicitud provocaría que superara el número de instantáneas permitido.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- SDK de AWS para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK de para Ruby V3

DeleteDBClusterParameterGroup

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Elimina un determinado grupo de parámetros de clúster especificados. El grupo de parámetros de clúster que se va a eliminar no puede asociarse a ningún clúster.

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

DBClusterParameterGroupName

El nombre del grupo de parámetros de clúster.

Restricciones:

- Debe ser el nombre de un grupo de parámetros de clúster existente.
- No puede eliminar un grupo de parámetros de clúster predeterminado.
- No se puede asociar con ningún clúster.

Tipo: cadena

Obligatorio: sí

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

DBParameterGroupNotFound

`DBParameterGroupName` no hace referencia a un grupo de parámetros existente.

Código de estado HTTP: 404

InvalidDBParameterGroupState

El grupo de parámetros está en uso o se encuentra en un estado que no es válido. Si intenta eliminar el grupo de parámetros, no puede eliminarlo cuando el grupo de parámetros se encuentra en este estado.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

DeleteDBClusterSnapshot

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Elimina una instantánea de clúster. Si se está copiando la instantánea, se termina la operación de copiado.

> **Note**
>
> La instantánea del clúster debe encontrarse en el estado `available` para su eliminación.

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

DBClusterSnapshotIdentifier

El identificador de la instantánea del clúster que se va a eliminar.

Restricciones: debe ser el nombre de una instantánea del clúster existente en el estado `available`.

Tipo: cadena

Obligatorio: sí

Elementos de respuesta

El servicio devuelve el siguiente elemento.

DBClusterSnapshot

Información detallada sobre una instantánea de un clúster.

Tipo: objeto DBClusterSnapshot

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

DBClusterSnapshotNotFoundFault

`DBClusterSnapshotIdentifier` no hace referencia a una instantánea de un clúster existente.

Código de estado HTTP: 404

InvalidDBClusterSnapshotStateFault

El valor proporcionado no es un estado de instantánea de clúster válido.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- SDK de AWS para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK de para Ruby V3

DeleteDBInstance

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Elimina una instancia previamente aprovisionada.

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

DBInstanceIdentifier

El identificador de instancias para la instancia que se va a eliminar. Este parámetro no distingue entre mayúsculas y minúsculas.

Restricciones:

- Debe coincidir con el nombre de una instancia existente.

Tipo: cadena

Obligatorio: sí

Elementos de respuesta

El servicio devuelve el siguiente elemento.

DBInstance

Información detallada sobre una instancia.

Tipo: objeto DBInstance

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

DBInstanceNotFound

`DBInstanceIdentifier` no hace referencia a una instancia existente.

Código de estado HTTP: 404

DBSnapshotAlreadyExists

Una instantánea existente ya está utilizando `DBSnapshotIdentifier`.

Código de estado HTTP: 400

InvalidDBClusterStateFault

El clúster no se encuentra en un estado válido.

Código de estado HTTP: 400

InvalidDBInstanceState

La instancia especificada no se encuentra en el estado disponible.

Código de estado HTTP: 400

SnapshotQuotaExceeded

La solicitud provocaría que superara el número de instantáneas permitido.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- SDK de AWS para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK de para Ruby V3

DeleteDBSubnetGroup

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Elimina un grupo de subredes.

> **Note**
>
> El grupo de subred de base de datos especificado no debe estar asociado a cualquier instancia de base de datos.

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

DBSubnetGroupName

El nombre del grupo de subred de base de datos que se va a eliminar.

> **Note**
>
> El grupo de subred predeterminado no se puede eliminar.

Restricciones:

Debe coincidir con el nombre de un existente `DBSubnetGroup`. No debe ser predeterminado.

Ejemplo:: `mySubnetgroup`

Tipo: cadena

Obligatorio: sí

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

DBSubnetGroupNotFoundFault

`DBSubnetGroupName` no hace referencia a un grupo de subredes existente.

Código de estado HTTP: 404

InvalidDBSubnetGroupStateFault

El grupo de subredes no se puede eliminar porque está en uso.

Código de estado HTTP: 400

InvalidDBSubnetStateFault

La subred de base de datos no se encuentra en el estado disponible.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- SDK de AWS para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK de para Ruby V3

DeleteEventSubscription

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Elimina una suscripción de notificación de eventos de Amazon DocumentDB.

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

SubscriptionName

El nombre de la suscripción a notificaciones de eventos de Amazon DocumentDB que desea eliminar.

Tipo: cadena

Obligatorio: sí

Elementos de respuesta

El servicio devuelve el siguiente elemento.

EventSubscription

Información detallada sobre un evento al que se ha suscrito.

Tipo: objeto EventSubscription

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidEventSubscriptionState

Es posible que otra persona esté modificando una suscripción. Espere unos segundos e inténtelo de nuevo.

Código de estado HTTP: 400

SubscriptionNotFound

El nombre de la suscripción no existe.

Código de estado HTTP: 404

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

DeleteGlobalCluster

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Elimina un clúster global. Los clústeres principal y secundario ya deben estar separados o eliminados antes de intentar eliminar un clúster global.

> **Note**
>
> Esta acción solo se aplica a los clústeres de Amazon DocumentDB.

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

GlobalClusterIdentifier

El identificador del clúster. del clúster global que se va a eliminar.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 255 caracteres.

Patrón: `[A-Za-z][0-9A-Za-z-:._]*`

Obligatorio: sí

Elementos de respuesta

El servicio devuelve el siguiente elemento.

GlobalCluster

Tipo de datos que representa un clúster global de Amazon DocumentDB.

Tipo: objeto GlobalCluster

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

GlobalClusterNotFoundFault

`GlobalClusterIdentifier` no hace referencia a un clúster global existente.

Código de estado HTTP: 404

InvalidGlobalClusterStateFault

La operación solicitada no se puede realizar mientras el clúster esté en este estado.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

DescribeCertificates

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Devuelve una lista de los certificados de la autoridad de certificación (CA) proporcionados por Amazon DocumentDB para esta Cuenta de AWS.

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

CertificateIdentifier

El identificador del certificado proporcionado por el usuario. Si se especifica este parámetro, se devuelve información solo del certificado especificado. Si se omite este parámetro, se devuelve una lista de hasta `MaxRecords` certificados. Este parámetro no distingue entre mayúsculas y minúsculas.

Restricciones

- Debe coincidir con un `CertificateIdentifier` existente.

Tipo: cadena

Requerido: no

Filters.Filter.N

Este parámetro es incompatible en estos momentos.

Tipo: matriz de objetos Filter

Obligatorio: no

Marker

Un token de paginación opcional proporcionado por una solicitud `DescribeCertificates` anterior. Si se especifica este parámetro, la respuesta solo incluye registros más allá del marcador, hasta el valor especificado por `MaxRecords`.

Tipo: cadena

Requerido: no

MaxRecords

El número máximo de registros que se deben incluir en la respuesta. Si el número de registros es superior al valor `MaxRecords` especificado, se incluye en la respuesta un token de paginación que se conoce como marcador, de modo que se pueda recuperar el resto de resultados.

Predeterminado: 100

Restricciones:

- Mínimo: 20
- Máximo: 100

Tipo: entero

Obligatorio: no

Elementos de respuesta

El servicio devuelve los siguientes elementos.

Certificates.Certificate.N

Una lista de certificados para esta Cuenta de AWS.

Tipo: matriz de objetos Certificate

Marker

Se proporciona un token de paginación opcional si el número de registros recuperados es superior a `MaxRecords`. Si se especifica este parámetro, el marcador especifica el siguiente registro de la lista. Si se incluye el valor de `Marker` en la siguiente llamada a `DescribeCertificates`, aparecerá la siguiente página de certificados.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

CertificateNotFound

`CertificateIdentifier` no hace referencia a un certificado existente.

Código de estado HTTP: 404

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

DescribeDBClusterParameterGroups

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Devuelve una lista de descripciones de `DBClusterParameterGroup`. Si se especifica un parámetro `DBClusterParameterGroupName`, la lista contendrá únicamente la descripción del grupo de parámetros de clúster especificado.

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

DBClusterParameterGroupName

El nombre de un grupo de parámetros de clúster específico para el que devolver detalles.

Restricciones:

- Si se suministra, debe coincidir con el nombre de un `DBClusterParameterGroup` existente.

Tipo: cadena

Requerido: no

Filters.Filter.N

Este parámetro es incompatible en estos momentos.

Tipo: matriz de objetos Filter

Obligatorio: no

Marker

Un token de paginación opcional proporcionado por una solicitud anterior. Si se especifica este parámetro, la respuesta solo incluye registros más allá del marcador, hasta el valor especificado por `MaxRecords`.

Tipo: cadena

Requerido: no

MaxRecords

El número máximo de registros que se deben incluir en la respuesta. Si el número de registros es superior al valor `MaxRecords` especificado, se incluye en la respuesta un token de paginación (marcador) de modo que se puedan recuperar el resto de los resultados.

Predeterminado: 100

Restricciones: mínimo 20, máximo 100.

Tipo: entero

Obligatorio: no

Elementos de respuesta

El servicio devuelve los siguientes elementos.

DBClusterParameterGroups.DBClusterParameterGroup.N

Una lista de grupos de parámetros de clúster.

Tipo: matriz de objetos DBClusterParameterGroup

Marker

Un token de paginación opcional proporcionado por una solicitud anterior. Si se especifica este parámetro, la respuesta solo incluye registros más allá del marcador, hasta el valor especificado por `MaxRecords`.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

DBParameterGroupNotFound

`DBParameterGroupName` no hace referencia a un grupo de parámetros existente.

Código de estado HTTP: 404

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

DescribeDBClusterParameters

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Devuelve la lista detallada de parámetros para un grupo de parámetros de clúster en particular.

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

DBClusterParameterGroupName

El nombre de un grupo de parámetros de clúster específico para el que devolver detalles de parámetros.

Restricciones:

- Si se suministra, debe coincidir con el nombre de un `DBClusterParameterGroup` existente.

Tipo: cadena

Obligatorio: sí

Filters.Filter.N

Este parámetro es incompatible en estos momentos.

Tipo: matriz de objetos Filter

Obligatorio: no

Marker

Un token de paginación opcional proporcionado por una solicitud anterior. Si se especifica este parámetro, la respuesta solo incluye registros más allá del marcador, hasta el valor especificado por `MaxRecords`.

Tipo: cadena

Requerido: no

MaxRecords

El número máximo de registros que se deben incluir en la respuesta. Si el número de registros es superior al valor `MaxRecords` especificado, se incluye en la respuesta un token de paginación (marcador) de modo que se puedan recuperar el resto de los resultados.

Predeterminado: 100

Restricciones: mínimo 20, máximo 100.

Tipo: entero

Obligatorio: no

Source

Un valor que indica devolver solo parámetros de un origen específico. Los orígenes de parámetros pueden ser `engine`, `service` o `customer`.

Tipo: cadena

Requerido: no

Elementos de respuesta

El servicio devuelve los siguientes elementos.

Marker

Un token de paginación opcional proporcionado por una solicitud anterior. Si se especifica este parámetro, la respuesta solo incluye registros más allá del marcador, hasta el valor especificado por `MaxRecords`.

Tipo: cadena

Parameters.Parameter.N

Proporciona una lista de parámetros para el grupo de parámetros de clúster.

Tipo: matriz de objetos Parameter

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

DBParameterGroupNotFound

`DBParameterGroupName` no hace referencia a un grupo de parámetros existente.

Código de estado HTTP: 404

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

DescribeDBClusters

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Devuelve información acerca de los clústeres de Amazon DocumentDB. La operación API admite la paginación. Para ciertas características de administración, como la administración del ciclo de vida de clúster y de instancia, Amazon DocumentDB aprovecha la tecnología operativa que se comparte con Amazon RDS and Amazon Neptune. Utilice el parámetro de filtro `filterName=engine,Values=docdb` para devolver únicamente los clústeres de Amazon DocumentDB.

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

DBClusterIdentifier

El identificador de clúster proporcionado por el usuario. Si se especifica este parámetro, se devuelve información solo del clúster específico. Este parámetro no distingue entre mayúsculas y minúsculas.

Restricciones:

- Si se suministra, debe coincidir con un `DBClusterIdentifier` existente.

Tipo: cadena

Requerido: no

Filters.Filter.N

Un filtro que especifica uno o varios clústeres por describir.

Filtros compatibles:

- `db-cluster-id`: acepta identificadores de clúster y clústeres de los Nombres de recursos de Amazon (ARN). La lista de resultados solo incluye información sobre los clústeres identificados por estos ARN.

Tipo: matriz de objetos Filter

Obligatorio: no

Marker

Un token de paginación opcional proporcionado por una solicitud anterior. Si se especifica este parámetro, la respuesta solo incluye registros más allá del marcador, hasta el valor especificado por `MaxRecords`.

Tipo: cadena

Requerido: no

MaxRecords

El número máximo de registros que se deben incluir en la respuesta. Si el número de registros es superior al valor `MaxRecords` especificado, se incluye en la respuesta un token de paginación (marcador) de modo que se puedan recuperar el resto de los resultados.

Predeterminado: 100

Restricciones: mínimo 20, máximo 100.

Tipo: entero

Obligatorio: no

Elementos de respuesta

El servicio devuelve los siguientes elementos.

DBClusters.DBCluster.N

Una lista de clústeres.

Tipo: matriz de objetos DBCluster

Marker

Un token de paginación opcional proporcionado por una solicitud anterior. Si se especifica este parámetro, la respuesta solo incluye registros más allá del marcador, hasta el valor especificado por `MaxRecords`.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

DBClusterNotFoundFault

`DBClusterIdentifier` no hace referencia a un clúster existente.

Código de estado HTTP: 404

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

DescribeDBClusterSnapshotAttributes

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Devuelve una lista de nombres y valores de atributos de instantáneas de clúster y valores para una instantánea del clúster de base de datos.

Cuando se comparten instantáneas con otras Cuentas de AWS, `DescribeDBClusterSnapshotAttributes` devuelve el atributo `restore` y una lista de ID de Cuentas de AWS que tienen autorización para copiar o restaurar la instantánea del clúster manual. Si `all` se incluye en la lista de valores para el atributo `restore`, la instantánea del clúster manual es pública y las Cuentas de AWS pueden copiarla o restaurarla.

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

DBClusterSnapshotIdentifier

El identificador para la instantánea del clúster para el que describir los atributos.

Tipo: cadena

Obligatorio: sí

Elementos de respuesta

El servicio devuelve el siguiente elemento.

DBClusterSnapshotAttributesResult

Información detallada sobre los atributos asociados a una instantánea de clúster.

Tipo: objeto DBClusterSnapshotAttributesResult

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

DBClusterSnapshotNotFoundFault

`DBClusterSnapshotIdentifier` no hace referencia a una instantánea de un clúster existente.

Código de estado HTTP: 404

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

DescribeDBClusterSnapshots

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Devuelve información acerca de instantáneas del clúster. La operación API admite la paginación.

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

DBClusterIdentifier

El ID del clúster para recuperar la lista de instantáneas del clúster. Este parámetro no puede utilizarse con el parámetro `DBClusterSnapshotIdentifier`. Este parámetro no distingue entre mayúsculas y minúsculas.

Restricciones:

- De ser proporcionado, debe coincidir con el identificador de un `DBCluster` existente.

Tipo: cadena

Requerido: no

DBClusterSnapshotIdentifier

Un identificador de instantánea de clúster específica para describir. Este parámetro no puede utilizarse con el parámetro `DBClusterIdentifier`. Este valor se almacena como una cadena en minúsculas.

Restricciones:

- De ser proporcionado, debe coincidir con el identificador de un `DBClusterSnapshot` existente.
- Si este identificador es para una instantánea automatizada, también se debe especificar el parámetro `SnapshotType`.

Tipo: cadena

Requerido: no

Filters.Filter.N

Este parámetro es incompatible en estos momentos.

Tipo: matriz de objetos Filter

Obligatorio: no

IncludePublic

Se establece en `true` para incluir instantáneas manuales del clúster que son públicas y que pueden ser copiadas o restauradas por cualquier Cuenta de AWS, o de otro modo `false`. El valor predeterminado es `false`.

Tipo: Booleano

Obligatorio: no

IncludeShared

Se establece en `true` para incluir instantáneas manuales compartidas del clúster de otras Cuentas de AWS a las que esta Cuenta de AWS ha recibido permiso para copiar o restaurar, y de otro modo `false`. El valor predeterminado es `false`.

Tipo: Booleano

Obligatorio: no

Marker

Un token de paginación opcional proporcionado por una solicitud anterior. Si se especifica este parámetro, la respuesta solo incluye registros más allá del marcador, hasta el valor especificado por `MaxRecords`.

Tipo: cadena

Requerido: no

MaxRecords

El número máximo de registros que se deben incluir en la respuesta. Si el número de registros es superior al valor `MaxRecords` especificado, se incluye en la respuesta un token de paginación (marcador) de modo que se puedan recuperar el resto de los resultados.

Predeterminado: 100

Restricciones: mínimo 20, máximo 100.

Tipo: entero

Obligatorio: no

SnapshotType

El tipo de instantáneas del clúster que se van a devolver. Puede especificar uno de los siguientes valores:

- `automated`: se devuelven todas las instantáneas del clúster que Amazon DocumentDB haya creado automáticamente para su Cuenta de AWS.
- `manual`: se devuelven todas las instantáneas del clúster que haya creado manualmente para su Cuenta de AWS.
- `shared`: se devuelven todas las instantáneas manuales del clúster que se han compartido a su Cuenta de AWS.
- `public`: se devuelven todas las instantáneas del clúster que se han marcado como públicas.

Si no se especifica ningún valor para `SnapshotType`, se devuelve las instantáneas del clúster automatizadas y manuales. Puede incluir instantáneas del clúster compartidas con estos resultados estableciendo el parámetro `IncludeShared` en `true`. Puede incluir instantáneas del clúster de base de datos públicas con estos resultados estableciendo el parámetro `IncludePublic` en `true`.

Los parámetros `IncludeShared` y `IncludePublic` no se aplican para los valores de `SnapshotType` de `manual` o `automated`. El parámetro `IncludePublic` no se aplica cuando se establece `SnapshotType` en `shared`. El parámetro `IncludeShared` no se aplica cuando se establece `SnapshotType` en `public`.

Tipo: cadena

Requerido: no

Elementos de respuesta

El servicio devuelve los siguientes elementos.

DBClusterSnapshots.DBClusterSnapshot.N

Proporciona una lista de instantáneas del clúster.

Tipo: matriz de objetos DBClusterSnapshot

Marker

Un token de paginación opcional proporcionado por una solicitud anterior. Si se especifica este parámetro, la respuesta solo incluye registros más allá del marcador, hasta el valor especificado por `MaxRecords`.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

DBClusterSnapshotNotFoundFault

`DBClusterSnapshotIdentifier` no hace referencia a una instantánea de un clúster existente.

Código de estado HTTP: 404

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- SDK de AWS para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK de para Ruby V3

DescribeDBEngineVersions

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Devuelve una lista con los motores disponibles.

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

DBParameterGroupFamily

El nombre de una familia de grupos de parámetros específicos para los que devolver detalles.

Restricciones:

- Si se suministra, debe coincidir con un `DBParameterGroupFamily` existente.

Tipo: cadena

Requerido: no

DefaultOnly

Indica que solo se devuelve la versión predeterminada del motor especificado o motor y combinación de la versión principal.

Tipo: Booleano

Obligatorio: no

Engine

El motor de base de datos que se debe devolver.

Tipo: cadena

Requerido: no

EngineVersion

La versión del motor de base de datos que se debe devolver.

Ejemplo:: `3.6.0`

Tipo: cadena

Requerido: no

Filters.Filter.N

Este parámetro es incompatible en estos momentos.

Tipo: matriz de objetos Filter

Obligatorio: no

ListSupportedCharacterSets

Si se especifica este parámetro y el motor solicitado es compatible con el parámetro `CharacterSetName` para `CreateDBInstance`, la respuesta incluye una lista de conjuntos de caracteres admitidos para cada versión del motor.

Tipo: Booleano

Obligatorio: no

ListSupportedTimezones

Si se especifica este parámetro y el motor solicitado es compatible con el parámetro `TimeZone` para `CreateDBInstance`, la respuesta incluye una lista de zonas horarias admitidas para cada versión del motor.

Tipo: Booleano

Obligatorio: no

Marker

Un token de paginación opcional proporcionado por una solicitud anterior. Si se especifica este parámetro, la respuesta solo incluye registros más allá del marcador, hasta el valor especificado por `MaxRecords`.

Tipo: cadena

Requerido: no

MaxRecords

El número máximo de registros que se deben incluir en la respuesta. Si el número de registros es superior al valor `MaxRecords` especificado, se incluye en la respuesta un token de paginación (marcador) de modo que se puedan recuperar el resto de los resultados.

Predeterminado: 100

Restricciones: mínimo 20, máximo 100.

Tipo: entero

Obligatorio: no

Elementos de respuesta

El servicio devuelve los siguientes elementos.

DBEngineVersions.DBEngineVersion.N

Información detallada sobre una o más versiones de un motor.

Tipo: matriz de objetos DBEngineVersion

Marker

Un token de paginación opcional proporcionado por una solicitud anterior. Si se especifica este parámetro, la respuesta solo incluye registros más allá del marcador, hasta el valor especificado por `MaxRecords`.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2

- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

DescribeDBInstances

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Devuelve información acerca de las instancias de Amazon DocumentDB aprovisionadas. Esta API admite la paginación.

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

DBInstanceIdentifier

El identificador de instancia proporcionado por el usuario. Si se especifica este parámetro, solo se devuelve información de la instancia específica. Este parámetro no distingue entre mayúsculas y minúsculas.

Restricciones:

- De ser proporcionado, debe coincidir con el identificador de un `DBInstance` existente.

Tipo: cadena

Requerido: no

Filters.Filter.N

Un filtro que especifica una o varias instancias para describir.

Filtros compatibles:

- `db-cluster-id`: acepta identificadores de clúster y clústeres de los Nombres de recursos de Amazon (ARN). La lista de resultados solo incluye información sobre las instancias asociadas con los clústeres identificados por estos ARN.
- `db-instance-id`: admite identificadores de instancia y ARN de instancia. La lista de resultados solo incluirá información sobre las instancias identificadas por estos ARN.

Tipo: matriz de objetos Filter

Obligatorio: no

Marker

Un token de paginación opcional proporcionado por una solicitud anterior. Si se especifica este parámetro, la respuesta solo incluye registros más allá del marcador, hasta el valor especificado por `MaxRecords`.

Tipo: cadena

Requerido: no

MaxRecords

El número máximo de registros que se deben incluir en la respuesta. Si el número de registros es superior al valor `MaxRecords` especificado, se incluye en la respuesta un token de paginación (marcador) de modo que se puedan recuperar el resto de los resultados.

Predeterminado: 100

Restricciones: mínimo 20, máximo 100.

Tipo: entero

Obligatorio: no

Elementos de respuesta

El servicio devuelve los siguientes elementos.

DBInstances.DBInstance.N

Información detallada sobre una o varias instancias.

Tipo: matriz de objetos DBInstance

Marker

Un token de paginación opcional proporcionado por una solicitud anterior. Si se especifica este parámetro, la respuesta solo incluye registros más allá del marcador, hasta el valor especificado por `MaxRecords`.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

DBInstanceNotFound

`DBInstanceIdentifier` no hace referencia a una instancia existente.

Código de estado HTTP: 404

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

DescribeDBSubnetGroups

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Devuelve una lista de descripciones de `DBSubnetGroup`. Si se especifica un `DBSubnetGroupName`, la lista contendrá únicamente la descripción del grupo de parámetros de `DBSubnetGroup` especificado.

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

DBSubnetGroupName

El nombre del grupo de subred del que desea consultar los detalles.

Tipo: cadena

Requerido: no

Filters.Filter.N

Este parámetro es incompatible en estos momentos.

Tipo: matriz de objetos Filter

Obligatorio: no

Marker

Un token de paginación opcional proporcionado por una solicitud anterior. Si se especifica este parámetro, la respuesta solo incluye registros más allá del marcador, hasta el valor especificado por `MaxRecords`.

Tipo: cadena

Requerido: no

MaxRecords

El número máximo de registros que se deben incluir en la respuesta. Si el número de registros es superior al valor `MaxRecords` especificado, se incluye en la respuesta un token de paginación (marcador) de modo que se puedan recuperar el resto de los resultados.

Predeterminado: 100

Restricciones: mínimo 20, máximo 100.

Tipo: entero

Obligatorio: no

Elementos de respuesta

El servicio devuelve los siguientes elementos.

DBSubnetGroups.DBSubnetGroup.N

Información detallada sobre uno o más grupos de subredes.

Tipo: matriz de objetos DBSubnetGroup

Marker

Un token de paginación opcional proporcionado por una solicitud anterior. Si se especifica este parámetro, la respuesta solo incluye registros más allá del marcador, hasta el valor especificado por `MaxRecords`.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

DBSubnetGroupNotFoundFault

`DBSubnetGroupName` no hace referencia a un grupo de subredes existente.

Código de estado HTTP: 404

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

DescribeEngineDefaultClusterParameters

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Devuelve la información de los parámetros del sistema y del motor predeterminados para el motor de base de datos del clúster.

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

DBParameterGroupFamily

El nombre de la familia del grupo de parámetros de clúster para la que devolver información de los parámetros del motor.

Tipo: cadena

Obligatorio: sí

Filters.Filter.N

Este parámetro es incompatible en estos momentos.

Tipo: matriz de objetos Filter

Obligatorio: no

Marker

Un token de paginación opcional proporcionado por una solicitud anterior. Si se especifica este parámetro, la respuesta solo incluye registros más allá del marcador, hasta el valor especificado por `MaxRecords`.

Tipo: cadena

Requerido: no

MaxRecords

El número máximo de registros que se deben incluir en la respuesta. Si el número de registros es superior al valor `MaxRecords` especificado, se incluye en la respuesta un token de paginación (marcador) de modo que se puedan recuperar el resto de los resultados.

Predeterminado: 100

Restricciones: mínimo 20, máximo 100.

Tipo: entero

Obligatorio: no

Elementos de respuesta

El servicio devuelve el siguiente elemento.

EngineDefaults

Contiene el resultado de una invocación correcta de la operación `DescribeEngineDefaultClusterParameters`.

Tipo: objeto EngineDefaults

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python

- AWS SDK para Ruby V3

DescribeEventCategories

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Muestra una lista de categorías de todos los tipos de origen de eventos o, si se especifica, para un tipo de origen especificado.

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

Filters.Filter.N

Este parámetro es incompatible en estos momentos.

Tipo: matriz de objetos Filter

Obligatorio: no

SourceType

El tipo de origen que está generando los eventos.

Valores válidos: `db-instance`, `db-parameter-group`, `db-security-group`

Tipo: cadena

Requerido: no

Elementos de respuesta

El servicio devuelve el siguiente elemento.

EventCategoriesMapList.EventCategoriesMap.N

Una lista de mapas de categorías de eventos.

Tipo: matriz de objetos EventCategoriesMap

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

DescribeEvents

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Devuelve eventos relacionados con las instancias, grupos de seguridad, instantáneas y grupos de parámetros de base de datos para los últimos 14 días. Los eventos específicos de una instancia de base de datos concreta, grupo de seguridad, instantánea o grupo de parámetros se pueden obtener proporcionando el nombre como parámetro. De forma predeterminada, se devuelven los eventos de la última hora.

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

Duration

El número de minutos para los que recuperar eventos.

Predeterminado: 60

Tipo: entero

Obligatorio: no

EndTime

El final del intervalo de tiempo para el que recuperar eventos, especificado en formato ISO 8601.

Ejemplo: 2009-07-08T18:00Z

Tipo: marca temporal

Obligatorio: no

EventCategories.EventCategory.N

Una lista de categorías de eventos que desencadena notificaciones para la suscripción a notificaciones de eventos.

Tipo: matriz de cadenas

Obligatorio: no

Filters.Filter.N

Este parámetro es incompatible en estos momentos.

Tipo: matriz de objetos Filter

Obligatorio: no

Marker

Un token de paginación opcional proporcionado por una solicitud anterior. Si se especifica este parámetro, la respuesta solo incluye registros más allá del marcador, hasta el valor especificado por `MaxRecords`.

Tipo: cadena

Requerido: no

MaxRecords

El número máximo de registros que se deben incluir en la respuesta. Si el número de registros es superior al valor `MaxRecords` especificado, se incluye en la respuesta un token de paginación (marcador) de modo que se puedan recuperar el resto de los resultados.

Predeterminado: 100

Restricciones: mínimo 20, máximo 100.

Tipo: entero

Obligatorio: no

SourceIdentifier

El identificador del origen de eventos para el que se devuelven eventos. Si no se especifica, se incluyen todos los orígenes en la respuesta.

Restricciones:

- Si se proporciona `SourceIdentifier`, también se debe proporcionar `SourceType`.
- Si el tipo de origen es `DBInstance`, debe proporcionarse un `DBInstanceIdentifier`.
- Si el tipo de origen es `DBSecurityGroup`, debe proporcionarse un `DBSecurityGroupName`.
- Si el tipo de origen es `DBParameterGroup`, debe proporcionarse un `DBParameterGroupName`.

- Si el tipo de origen es `DBSnapshot`, debe proporcionarse un `DBSnapshotIdentifier`.
- No puede terminar por un guion ni contener dos guiones consecutivos.

Tipo: cadena

Requerido: no

SourceType

El origen del evento para el que recuperar eventos. Si no se especifica ningún valor, se devuelven todos los eventos.

Tipo: cadena

Valores válidos: `db-instance | db-parameter-group | db-security-group | db-snapshot | db-cluster | db-cluster-snapshot`

Obligatorio: no

StartTime

El principio del intervalo de tiempo para el que recuperar eventos, especificado en formato ISO 8601.

Ejemplo: 2009-07-08T18:00Z

Tipo: marca temporal

Obligatorio: no

Elementos de respuesta

El servicio devuelve los siguientes elementos.

Events.Event.N

Información detallada sobre uno o varios eventos.

Tipo: matriz de objetos Event

Marker

Un token de paginación opcional proporcionado por una solicitud anterior. Si se especifica este parámetro, la respuesta solo incluye registros más allá del marcador, hasta el valor especificado por `MaxRecords`.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

DescribeEventSubscriptions

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Muestra todas las descripciones de la suscripción para una cuenta de cliente. La descripción de una suscripción incluye `SubscriptionName`, `SNSTopicARN`, `CustomerID`, `SourceType`, `SourceID`, `CreationTime` y `Status`.

Si especifica un `SubscriptionName`, muestra la descripción de dicha suscripción.

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

Filters.Filter.N

Este parámetro es incompatible en estos momentos.

Tipo: matriz de objetos Filter

Obligatorio: no

Marker

Un token de paginación opcional proporcionado por una solicitud anterior. Si se especifica este parámetro, la respuesta solo incluye registros más allá del marcador, hasta el valor especificado por `MaxRecords`.

Tipo: cadena

Requerido: no

MaxRecords

El número máximo de registros que se deben incluir en la respuesta. Si el número de registros es superior al valor `MaxRecords` especificado, se incluye en la respuesta un token de paginación (marcador) de modo que se puedan recuperar el resto de los resultados.

Predeterminado: 100

Restricciones: mínimo 20, máximo 100.

Tipo: entero

Obligatorio: no

SubscriptionName

El nombre de la suscripción a notificaciones de eventos de Amazon DocumentDB que desea describir.

Tipo: cadena

Requerido: no

Elementos de respuesta

El servicio devuelve los siguientes elementos.

EventSubscriptionsList.EventSubscription.N

Lista de suscripciones a eventos.

Tipo: matriz de objetos EventSubscription

Marker

Un token de paginación opcional proporcionado por una solicitud anterior. Si se especifica este parámetro, la respuesta solo incluye registros más allá del marcador, hasta el valor especificado por `MaxRecords`.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

SubscriptionNotFound

El nombre de la suscripción no existe.

Código de estado HTTP: 404

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

DescribeGlobalClusters

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Devuelve información sobre los clústeres globales de Amazon DocumentDB. Esta API admite la paginación.

> **Note**
>
> Esta acción solo se aplica a los clústeres de Amazon DocumentDB.

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

Filters.Filter.N

Un filtro que especifica uno o varios clústeres de bases de datos globales a describir.

Filtros admitidos: `db-cluster-id` acepta identificadores de clúster y Nombres de recursos de Amazon (ARN) de clúster. La lista de resultados solo incluirá información sobre los clústeres identificados por estos ARN.

Tipo: matriz de objetos Filter

Obligatorio: no

GlobalClusterIdentifier

El identificador de clúster de base de datos suministrado por el usuario. Si se especifica este parámetro, se devuelve información solo del clúster específico. Este parámetro no distingue entre mayúsculas y minúsculas.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 255 caracteres.

Patrón: `[A-Za-z][0-9A-Za-z-:._]*`

Obligatorio: no

Marker

Un token de paginación opcional proporcionado por una solicitud `DescribeGlobalClusters` anterior. Si se especifica este parámetro, la respuesta solo incluye registros más allá del marcador, hasta el valor especificado por `MaxRecords`.

Tipo: cadena

Requerido: no

MaxRecords

El número máximo de registros que se deben incluir en la respuesta. Si el número de registros es superior al valor `MaxRecords` especificado, se incluye en la respuesta un token de paginación que se conoce como marcador, de modo que usted pueda recuperar el resto de los resultados.

Tipo: entero

Obligatorio: no

Elementos de respuesta

El servicio devuelve los siguientes elementos.

GlobalClusters.GlobalClusterMember.N

Tipo: matriz de objetos GlobalCluster

Marker

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

GlobalClusterNotFoundFault

`GlobalClusterIdentifier` no hace referencia a un clúster global existente.

Código de estado HTTP: 404

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

DescribeOrderableDBInstanceOptions

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Devuelve una lista de opciones de instancia ordenable para el motor especificado.

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

Engine

Nombre del motor para recuperar opciones de la instancia.

Tipo: cadena

Obligatorio: sí

DBInstanceClass

El valor del filtro de la clase de instancia. Especifique este parámetro para mostrar solo las ofertas disponibles que coinciden con la clase de instancia especificada.

Tipo: cadena

Requerido: no

EngineVersion

Valor del filtro de la versión del motor. Especifique este parámetro para mostrar solo las ofertas disponibles que coinciden con la versión del motor especificado.

Tipo: cadena

Requerido: no

Filters.Filter.N

Este parámetro es incompatible en estos momentos.

Tipo: matriz de objetos Filter

Obligatorio: no

LicenseModel

El valor del filtro del modelo de licencia. Especifique este parámetro para mostrar solo las ofertas disponibles que coinciden con el modelo de licencia especificado.

Tipo: cadena

Requerido: no

Marker

Un token de paginación opcional proporcionado por una solicitud anterior. Si se especifica este parámetro, la respuesta solo incluye registros más allá del marcador, hasta el valor especificado por `MaxRecords`.

Tipo: cadena

Requerido: no

MaxRecords

El número máximo de registros que se deben incluir en la respuesta. Si el número de registros es superior al valor `MaxRecords` especificado, se incluye en la respuesta un token de paginación (marcador) de modo que se puedan recuperar el resto de los resultados.

Predeterminado: 100

Restricciones: mínimo 20, máximo 100.

Tipo: entero

Obligatorio: no

Vpc

Valor del filtro de la nube privada virtual (VPC). Especifique este parámetro para mostrar solo la disponibilidad de ofertas VPC o no VPC.

Tipo: Booleano

Obligatorio: no

Elementos de respuesta

El servicio devuelve los siguientes elementos.

Marker

Un token de paginación opcional proporcionado por una solicitud anterior. Si se especifica este parámetro, la respuesta solo incluye registros más allá del marcador, hasta el valor especificado por `MaxRecords`.

Tipo: cadena

OrderableDBInstanceOptions.OrderableDBInstanceOption.N

Las opciones que están disponibles para una instancia concreta que se puede pedir.

Tipo: matriz de objetos OrderableDBInstanceOption

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

DescribePendingMaintenanceActions

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Devuelve una lista de recursos (por ejemplo, instancias) que tienen al menos una acción de mantenimiento pendiente.

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

Filters.Filter.N

Un filtro que especifica uno o más recursos para devolver acciones de mantenimiento pendientes.

Filtros compatibles:

- `db-cluster-id`: acepta identificadores de clúster y clústeres de los Nombres de recursos de Amazon (ARN). La lista de resultados solo incluye las acciones de mantenimiento pendientes para los clústeres identificados por estos ARN.
- `db-instance-id`: admite identificadores de instancia y ARN de instancia. La lista de resultados solo incluye las acciones de mantenimiento pendientes para las instancias de base de datos identificadas por estos ARN.

Tipo: matriz de objetos Filter

Obligatorio: no

Marker

Un token de paginación opcional proporcionado por una solicitud anterior. Si se especifica este parámetro, la respuesta solo incluye registros más allá del marcador, hasta el valor especificado por `MaxRecords`.

Tipo: cadena

Requerido: no

MaxRecords

El número máximo de registros que se deben incluir en la respuesta. Si el número de registros es superior al valor `MaxRecords` especificado, se incluye en la respuesta un token de paginación (marcador) de modo que se puedan recuperar el resto de los resultados.

Predeterminado: 100

Restricciones: mínimo 20, máximo 100.

Tipo: entero

Obligatorio: no

ResourceIdentifier

El ARN de un recuerdo para el que devolver acciones de mantenimiento pendientes.

Tipo: cadena

Requerido: no

Elementos de respuesta

El servicio devuelve los siguientes elementos.

Marker

Un token de paginación opcional proporcionado por una solicitud anterior. Si se especifica este parámetro, la respuesta solo incluye registros más allá del marcador, hasta el valor especificado por `MaxRecords`.

Tipo: cadena

PendingMaintenanceActions.ResourcePendingMaintenanceActions.N

Las acciones de mantenimiento que se van a aplicar.

Tipo: matriz de objetos ResourcePendingMaintenanceActions

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

ResourceNotFoundFault

No se ha encontrado el ID del recurso especificado.

Código de estado HTTP: 404

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

FailoverDBCluster

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Fuerza una conmutación por error para un clúster.

Una conmutación por error de un clúster promueve una de las réplicas de Amazon DocumentDB (instancias de solo lectura) del clúster a instancia principal (la instancia de escritura del clúster).

Si se produce un error en la instancia principal, Amazon DocumentDB conmuta automáticamente a una réplica de Amazon DocumentDB, si existe. Puede forzar una conmutación por error cuando desee simular un error en una instancia principal para realizar pruebas.

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

DBClusterIdentifier

Un identificador del clúster para forzar una conmutación por error. Este parámetro no distingue entre mayúsculas y minúsculas.

Restricciones:

- Debe coincidir con el identificador de un `DBCluster` existente.

Tipo: cadena

Requerido: no

TargetDBInstanceIdentifier

El nombre de la instancia que se va a promover a instancia principal.

Debe especificar el identificador de instancias para una réplica de Amazon DocumentDB en el clúster. Por ejemplo, `mydbcluster-replica1`.

Tipo: cadena

Requerido: no

Elementos de respuesta

El servicio devuelve el siguiente elemento.

DBCluster

Información detallada sobre un clúster.

Tipo: objeto DBCluster

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

DBClusterNotFoundFault

`DBClusterIdentifier` no hace referencia a un clúster existente.

Código de estado HTTP: 404

InvalidDBClusterStateFault

El clúster no se encuentra en un estado válido.

Código de estado HTTP: 400

InvalidDBInstanceState

La instancia especificada no se encuentra en el estado disponible.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- SDK de AWS para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin

- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK de para Ruby V3

FailoverGlobalCluster

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Hace que el clúster de base de datos secundario especificado sea el clúster de base de datos principal del clúster global cuando se produce una conmutación por error en un clúster global.

Utilice esta operación para responder a un suceso no planificado, como un desastre regional en la región principal. La conmutación por error puede provocar la pérdida de datos de transacciones de escritura que no se replicaron en el clúster secundario elegido antes de que se produjera el evento de conmutación por error. Sin embargo, el proceso de recuperación que promueve una instancia de base de datos del clúster de base de datos secundario elegido a instancia de base de datos principal de escritura garantiza que el estado de los datos sea coherente desde el punto de vista de las transacciones.

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

GlobalClusterIdentifier

El identificador del clúster global de Amazon DocumentDB para aplicar esta operación. El identificador es la clave única asignada por el usuario cuando se creó el clúster. Dicho de otro modo, es el nombre del clúster global.

Restricciones:

- Debe coincidir con el identificador de un clúster existente.
- Longitud mínima de 1. La longitud máxima es de 255 caracteres.

Patrón: `[A-Za-z][0-9A-Za-z-:._]*`

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 255 caracteres.

Patrón: `[A-Za-z][0-9A-Za-z-:._]*`

Obligatorio: sí

TargetDbClusterIdentifier

El identificador del clúster secundario de Amazon DocumentDB que desea promover para que sea el principal del clúster global. Utilice el Nombre de recurso de Amazon (ARN) para el identificador de modo que Amazon DocumentDB pueda localizar el clúster en su región de AWS.

Restricciones:

- Debe coincidir con el identificador de un clúster secundario existente.
- Longitud mínima de 1. La longitud máxima es de 255 caracteres.

Patrón: `[A-Za-z][0-9A-Za-z-:._]*`

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 255 caracteres.

Patrón: `[A-Za-z][0-9A-Za-z-:._]*`

Obligatorio: sí

AllowDataLoss

Especifica si se debe permitir la pérdida de datos para esta operación de clúster global. Al permitir la pérdida de datos, se desencadena una operación de conmutación por error global.

Si no especifica `AllowDataLoss`, la operación del clúster global se establece de forma predeterminada en una transición.

Restricciones:

- No se puede especificar junto con el parámetro `Switchover`.

Tipo: Booleano

Obligatorio: no

Switchover

Especifica si se debe hacer la transición de este clúster de base de datos global.

Restricciones:

- No se puede especificar junto con el parámetro `AllowDataLoss`.

Tipo: Booleano

Obligatorio: no

Elementos de respuesta

El servicio devuelve el siguiente elemento.

GlobalCluster

Tipo de datos que representa un clúster global de Amazon DocumentDB.

Tipo: objeto GlobalCluster

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

DBClusterNotFoundFault

`DBClusterIdentifier` no hace referencia a un clúster existente.

Código de estado HTTP: 404

GlobalClusterNotFoundFault

`GlobalClusterIdentifier` no hace referencia a un clúster global existente.

Código de estado HTTP: 404

InvalidDBClusterStateFault

El clúster no se encuentra en un estado válido.

Código de estado HTTP: 400

InvalidGlobalClusterStateFault

La operación solicitada no se puede realizar mientras el clúster esté en este estado.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

ListTagsForResource

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Enumera todas las etiquetas de un recurso de Amazon DocumentDB.

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

ResourceName

El recurso de Amazon DocumentDB con las etiquetas que se desea listar. Este valor es un Nombre de recurso de Amazon (ARN).

Tipo: cadena

Obligatorio: sí

Filters.Filter.N

Este parámetro es incompatible en estos momentos.

Tipo: matriz de objetos Filter

Obligatorio: no

Elementos de respuesta

El servicio devuelve el siguiente elemento.

TagList.Tag.N

Una lista de una o varias etiquetas.

Tipo: matriz de objetos Tag

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

DBClusterNotFoundFault

`DBClusterIdentifier` no hace referencia a un clúster existente.

Código de estado HTTP: 404

DBInstanceNotFound

`DBInstanceIdentifier` no hace referencia a una instancia existente.

Código de estado HTTP: 404

DBSnapshotNotFound

`DBSnapshotIdentifier` no hace referencia a una instantánea existente.

Código de estado HTTP: 404

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

ModifyDBCluster

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Modifica un ajuste para un clúster de Amazon DocumentDB. Puede cambiar uno o varios parámetros de configuración de la base de datos mediante la especificación de estos parámetros y los nuevos valores en la solicitud.

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

DBClusterIdentifier

El identificador del clúster que se está modificando. Este parámetro no distingue entre mayúsculas y minúsculas.

Restricciones:

- Debe coincidir con el identificador de un `DBCluster` existente.

Tipo: cadena

Obligatorio: sí

AllowMajorVersionUpgrade

Es un valor que indica si se permiten actualizaciones de las versiones principales.

Restricciones:

- Debe permitir las actualizaciones de la versión principal cuando especifique un valor para el parámetro `EngineVersion` que sea una versión principal diferente a la versión actual del clúster.
- Dado que algunos parámetros son específicos de la versión, cambiarlos requiere ejecutar una nueva llamada a la API `ModifyDBCluster` una vez que se complete la MVU local.

> **Note**
>
> La ejecución de una MVU afecta directamente los siguientes parámetros:
>
> - `MasterUserPassword`
> - `NewDBClusterIdentifier`

- `VpcSecurityGroupIds`
- `Port`

Tipo: Booleano

Obligatorio: no

ApplyImmediately

Un valor que especifica si los cambios de esta solicitud y todos los cambios pendientes se asignan de manera asincrónica en cuanto sea posible, independientemente del valor de `PreferredMaintenanceWindow` del clúster. Si este parámetro es `false`, los cambios realizados en el clúster se aplican durante la siguiente ventana de mantenimiento.

El parámetro `ApplyImmediately` solo afecta a los valores `NewDBClusterIdentifier` y `MasterUserPassword`. Si ajusta el valor de este parámetro a `false`, los cambios en los valores `NewDBClusterIdentifier` y `MasterUserPassword` se aplicarán durante la siguiente ventana de mantenimiento. Todas los demás cambios se aplican de inmediato, con independencia del valor del parámetro `ApplyImmediately`.

Predeterminado: `false`

Tipo: Booleano

Obligatorio: no

BackupRetentionPeriod

El número de días durante los que se retienen las copias de seguridad automatizadas. Debe especificar un valor mínimo de 1.

Valor predeterminado: 1

Restricciones:

- Debe ser un valor entre 1 y 35.

Tipo: entero

Obligatorio: no

CloudwatchLogsExportConfiguration

La opción de configuración para los tipos de registro que se debe habilitar para la exportación a Registros de Amazon CloudWatch para una instancia o un clúster específico. Las matrices `EnableLogTypes` y `DisableLogTypes` determinan qué registros se exportarán (o no) a CloudWatch Logs.

Tipo: objeto CloudwatchLogsExportConfiguration

Obligatorio: no

DBClusterParameterGroupName

El nombre del grupo de parámetros de clúster que se va a usar para el clúster.

Tipo: cadena

Requerido: no

DeletionProtection

Especifica si se puede eliminar este clúster. Si `DeletionProtection` está habilitado, no se puede eliminar el clúster a menos que se modifique y `DeletionProtection` esté deshabilitado. `DeletionProtection` protege los clústeres de una eliminación accidental.

Tipo: Booleano

Obligatorio: no

EngineVersion

El número de versión del motor de base de datos al que desea realizar la actualización. El cambio de este parámetro produce una interrupción. El cambio se aplica durante la siguiente ventana de mantenimiento a menos que `ApplyImmediately` esté activado.

Para listar todas las versiones de motor disponibles para Amazon DocumentDB utilice el siguiente comando:

```
aws docdb describe-db-engine-versions --engine docdb --query
"DBEngineVersions[].EngineVersion"
```

Tipo: cadena

Requerido: no

ManageMasterUserPassword

Especifica si se debe administrar la contraseña del usuario maestro con Secrets Manager de Amazon Web Services. Si el clúster no administra la contraseña del usuario maestro con Secrets Manager de Amazon Web Services, puede activar esta administración. En este caso, no puede especificar `MasterUserPassword`. Si el clúster ya administra la contraseña del usuario maestro con Secrets Manager de Amazon Web Services y usted especifica que la contraseña del usuario maestro no se administre con Secrets Manager de Amazon Web Services, debe especificar `MasterUserPassword`. En este caso, Amazon DocumentDB elimina el secreto y utiliza la nueva contraseña para el usuario maestro especificado por `MasterUserPassword`.

Tipo: Booleano

Obligatorio: no

MasterUserPassword

La contraseña del usuario de la base de datos maestra. Esta contraseña puede contener cualquier carácter ASCII imprimible, excepto barra inclinada (/), comillas dobles (") o el símbolo de “arroba” (@).

Limitaciones: debe contener de 8 a 100 caracteres.

Tipo: cadena

Requerido: no

MasterUserSecretKmsKeyId

El identificador de clave KMS de Amazon Web Services para cifrar un secreto que se genera y administra automáticamente en Secrets Manager de Amazon Web Services.

Esta configuración es válida solamente si se cumplen las siguientes dos condiciones:

- Si el clúster no administra la contraseña del usuario maestro con Secrets Manager de Amazon Web Services. Si el clúster ya administra la contraseña de usuario maestro en Secrets Manager de Amazon Web Services, no podrá cambiar la clave de KMS que se usa para cifrar el secreto.
- Está habilitando `ManageMasterUserPassword` para que administre la contraseña de usuario maestro en Secrets Manager de Amazon Web Services. Si activa `ManageMasterUserPassword` y no especifica el `MasterUserSecretKmsKeyId`, se utilizará la clave de KMS de `aws/secretsmanager` para cifrar el secreto. Si el secreto está en una cuenta de Amazon Web Services diferente, entonces no puede usar la clave de KMS de `aws/`

`secretsmanager` para cifrar el secreto y se debe usar una clave de KMS administrada por el cliente.

El identificador de la clave de KMS de Amazon Web Services es el ARN de la clave, el identificador de clave, el ARN de alias o el nombre de alias de la clave de KMS. Para utilizar una clave de KMS en una cuenta de Amazon Web Services diferente, debe especificar el ARN de la clave o el ARN del alias.

Existe una clave KMS predeterminada para su cuenta de Amazon Web Services. La cuenta de Amazon Web Services tiene una clave de KMS predeterminada diferente para cada región de Amazon Web Services.

Tipo: cadena

Requerido: no

NetworkType

El tipo de red del clúster.

El tipo de red viene determinado por el `DBSubnetGroup` especificado para el clúster. Un `DBSubnetGroup` admite solamente el protocolo IPv4 o los protocolos IPv4 e IPv6 (`DUAL`).

Para obtener más información, consulte Clústeres de DocumentDB en una VPC en la Guía para desarrolladores de Amazon DocumentDB.

Valores válidos: `IPV4` | `DUAL`

Tipo: cadena

Requerido: no

NewDBClusterIdentifier

El nuevo identificador del clúster cuando se cambia el nombre de un clúster. Este valor se almacena como una cadena en minúsculas.

Restricciones:

- Deben contener de 1 a 63 caracteres (letras, números o guiones).
- El primer carácter debe ser una letra.
- No puede terminar por un guion ni contener dos guiones consecutivos.

Ejemplo:: `my-cluster2`

Tipo: cadena

Requerido: no

Port

El número de puerto en el que el clúster acepta las conexiones.

Restricciones: el valor debe estar entre `1150` y `65535`.

Valor predeterminado: el mismo puerto que el clúster original.

Tipo: entero

Obligatorio: no

PreferredBackupWindow

El intervalo de tiempo diario durante el que se crean las copias de seguridad automatizadas si las copias de seguridad automatizadas están habilitadas con el parámetro `BackupRetentionPeriod`.

El valor predeterminado es una ventana de 30 minutos seleccionada al azar dentro de un bloque de 8 horas para cada Región de AWS.

Restricciones:

- Tiene que tener el formato `hh24:mi-hh24:mi`.
- Debe indicarse en Tiempo universal coordinado (UTC).
- No debe entrar en conflicto con la ventana de mantenimiento preferida.
- Debe durar al menos 30 minutos.

Tipo: cadena

Requerido: no

PreferredMaintenanceWindow

El intervalo de tiempo semanal durante el cual puede llevarse a cabo el mantenimiento del sistema, en tiempo universal coordinado (UTC).

Formato: `ddd:hh24:mi-ddd:hh24:mi`

El valor predeterminado es un periodo de 30 minutos seleccionado al azar de un bloque de 8 horas de tiempo para cada Región de AWS, que tiene lugar un día de la semana al azar.

Días válidos: lunes, martes, miércoles, jueves, viernes, sábado, domingo

Restricciones: ventana mínima de 30 minutos.

Tipo: cadena

Requerido: no

RotateMasterUserPassword

Especifica si se debe rotar el secreto administrado por Secrets Manager de Amazon Web Services para la contraseña del usuario maestro.

Esta configuración solo es válida si Amazon DocumentDB administra la contraseña del usuario maestro en Secrets Manager de Amazon Web Services para el clúster. El valor del secreto contiene la contraseña actualizada.

Restricción: debe aplicar el cambio inmediatamente cuando rota la contraseña del usuario maestro.

Tipo: Booleano

Obligatorio: no

ServerlessV2ScalingConfiguration

Contiene la configuración de escalado de un clúster de Amazon DocumentDB sin servidor.

Tipo: objeto ServerlessV2ScalingConfiguration

Obligatorio: no

StorageType

El tipo de almacenamiento que se va a asociar al clúster de base de datos.

Para obtener información sobre los tipos de almacenamiento de los clústeres de Amazon DocumentDB, consulte Cluster storage configurations en la Guía para desarrolladores de Amazon DocumentDB.

Valores válidos para el tipo de almacenamiento: `standard | iopt1`

El valor predeterminado es `standard`

Tipo: cadena

Requerido: no

VpcSecurityGroupIds.VpcSecurityGroupId.N

Una lista de grupos de seguridad de la nube privada virtual (VPC) a la que pertenecerá el clúster.

Tipo: matriz de cadenas

Obligatorio: no

Elementos de respuesta

El servicio devuelve el siguiente elemento.

DBCluster

Información detallada sobre un clúster.

Tipo: objeto DBCluster

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

DBClusterAlreadyExistsFault

El usuario ya tiene un clúster con el identificador concreto.

Código de estado HTTP: 400

DBClusterNotFoundFault

`DBClusterIdentifier` no hace referencia a un clúster existente.

Código de estado HTTP: 404

DBClusterParameterGroupNotFound

`DBClusterParameterGroupName` no hace referencia a un grupo de parámetros de clúster existente.

Código de estado HTTP: 404

DBSubnetGroupNotFoundFault

DBSubnetGroupName no hace referencia a un grupo de subredes existente.

Código de estado HTTP: 404

InvalidDBClusterStateFault

El clúster no se encuentra en un estado válido.

Código de estado HTTP: 400

InvalidDBInstanceState

La instancia especificada no se encuentra en el estado disponible.

Código de estado HTTP: 400

InvalidDBSecurityGroupState

El estado del grupo de seguridad no permite la eliminación.

Código de estado HTTP: 400

InvalidDBSubnetGroupStateFault

El grupo de subredes no se puede eliminar porque está en uso.

Código de estado HTTP: 400

InvalidSubnet

La subred solicitada no es válida o se solicitaron varias subredes que no están en la misma nube privada virtual (VPC).

Código de estado HTTP: 400

InvalidVPCNetworkStateFault

El grupo de subredes no cubre todas las zonas de disponibilidad después de crearla, debido a los cambios realizados.

Código de estado HTTP: 400

NetworkTypeNotSupported

El tipo de red no es compatible con DBSubnetGroup ni con la versión del motor de base de datos.

Código de estado HTTP: 400

StorageQuotaExceeded

La solicitud provocaría que superara la cantidad permitida de almacenamiento disponible en todas las instancias.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

ModifyDBClusterParameterGroup

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Modifica los parámetros de un grupo de parámetros de clúster. Para modificar más de un parámetro, envíe una lista de los siguientes: `ParameterName`, `ParameterValue` y `ApplyMethod`. Se pueden modificar un máximo de 20 parámetros en una única solicitud.

> **Note**
>
> Los cambios realizados en los parámetros dinámicos se aplican inmediatamente. Los cambios en los parámetros estáticos requieren un período de reinicio o mantenimiento antes de que el cambio pueda surtir efecto.

> **Important**
>
> Después de crear un grupo de parámetros de clúster, debe esperar al menos 5 minutos antes de crear el primer clúster que utilice ese grupo de parámetros de clúster como grupo de parámetros predeterminado. Esto permite a Amazon DocumentDB finalizar por completo la acción de creación antes de que el grupo de parámetros de clúster se use de forma predeterminada para un clúster nuevo. Este paso es especialmente importante para los parámetros que son críticos al crear la base de datos predeterminada de un clúster, como el conjunto de caracteres de la base de datos predeterminada definido por el parámetro `character_set_database`.

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

DBClusterParameterGroupName

El nombre del grupo de parámetros de clúster que se va a modificar.

Tipo: cadena

Obligatorio: sí

Parameters.Parameter.N

Un lista de parámetros en el grupo de parámetros de clúster que se va a modificar.

Tipo: matriz de objetos Parameter

Obligatorio: sí

Elementos de respuesta

El servicio devuelve el siguiente elemento.

DBClusterParameterGroupName

El nombre del grupo de parámetros de clúster.

Restricciones:

- Debe tener de 1 a 255 letras o números.
- El primer carácter debe ser una letra.
- No puede terminar por un guion ni contener dos guiones consecutivos.

> **Note**
>
> Este valor se almacena como una cadena en minúsculas.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

DBParameterGroupNotFound

`DBParameterGroupName` no hace referencia a un grupo de parámetros existente.

Código de estado HTTP: 404

InvalidDBParameterGroupState

El grupo de parámetros está en uso o se encuentra en un estado que no es válido. Si intenta eliminar el grupo de parámetros, no puede eliminarlo cuando el grupo de parámetros se encuentra en este estado.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

ModifyDBClusterSnapshotAttribute

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Añade un atributo y valores a una instantánea manual del clúster de base de datos o los elimina.

Para compartir una instantánea manual del clúster con otras Cuentas de AWS, especifique `restore` como `AttributeName` y utilice el parámetro `ValuesToAdd` para añadir una lista de ID de las Cuentas de AWS autorizadas a restaurar la instantánea manual del clúster. Utilice el valor `all` para convertir la instantánea manual del clúster en pública, lo que significa que todas las Cuentas de AWS la pueden copiar o restaurar. No añada el valor `all` a ninguna instantánea manual del clúster que contenga información privada que no quiera que esté disponible para todas las Cuentas de AWS. Si una instantánea manual del clúster está cifrada, se podrá compartir, pero solo especificando una lista de ID de Cuenta de AWS autorizados para el parámetro `ValuesToAdd`. No se puede utilizar `all` como valor para ese parámetro en este caso.

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

AttributeName

El nombre del atributo de la instantánea del clúster que se va a modificar.

Para administrar la autorización para otras Cuentas de AWS para copiar o restaurar una instantánea manual del clúster, establezca este valor en `restore`.

Tipo: cadena

Obligatorio: sí

DBClusterSnapshotIdentifier

El identificador para la instantánea del clúster para el que se modifican los atributos.

Tipo: cadena

Obligatorio: sí

ValuesToAdd.AttributeValue.N

Una lista de atributos de la instantánea del clúster que desea añadir al atributo especificado por `AttributeName`.

Para autorizar a otras Cuentas de AWS a copiar o restaurar una instantánea de clúster manual, configure esta lista para que incluya uno o más ID de Cuenta de AWS. Para que cualquier Cuenta de AWS pueda restaurar la instantánea manual del clúster, configúrela en `all`. No añada el valor `all` a ninguna instantánea manual del clúster que contenga información privada que no quiera que esté disponible para todas las Cuentas de AWS.

Tipo: matriz de cadenas

Obligatorio: no

ValuesToRemove.AttributeValue.N

Una lista de atributos de la instantánea del clúster que desea eliminar del atributo especificado por `AttributeName`.

Para eliminar la autorización para que otras Cuentas de AWS copien o restauren una instantánea de clúster manual, configure esta lista para que incluya uno o más identificadores de Cuenta de AWS. Para eliminar la autorización para que cualquier Cuenta de AWS copie o restaure la instantánea del clúster, configúrela en `all`. Si especifica `all`, una Cuenta de AWS cuyo ID de cuenta se añade explícitamente al atributo `restore` puede seguir copiando o restaurando una instantánea manual del clúster.

Tipo: matriz de cadenas

Obligatorio: no

Elementos de respuesta

El servicio devuelve el siguiente elemento.

DBClusterSnapshotAttributesResult

Información detallada sobre los atributos asociados a una instantánea de clúster.

Tipo: objeto DBClusterSnapshotAttributesResult

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

DBClusterSnapshotNotFoundFault

`DBClusterSnapshotIdentifier` no hace referencia a una instantánea de un clúster existente.

Código de estado HTTP: 404

InvalidDBClusterSnapshotStateFault

El valor proporcionado no es un estado de instantánea de clúster válido.

Código de estado HTTP: 400

SharedSnapshotQuotaExceeded

Ha superado el número máximo de cuentas con las que puede compartir una instantánea manual de base de datos.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

ModifyDBInstance

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Modifica la configuración de una instancia. Puede cambiar uno o varios parámetros de configuración de la base de datos mediante la especificación de estos parámetros y los nuevos valores en la solicitud.

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

DBInstanceIdentifier

El identificador de instancias. Este valor se almacena como una cadena en minúsculas.

Restricciones:

- Debe coincidir con el identificador de un existente `DBInstance`.

Tipo: cadena

Obligatorio: sí

ApplyImmediately

Especifica si las modificaciones de esta solicitud y todas las modificaciones pendientes se aplican de manera asíncrona en cuanto es posible, independientemente de la configuración de `PreferredMaintenanceWindow` de esta instancia.

Si este parámetro se establece en `false`, los cambios realizados en la instancia se aplican durante la siguiente ventana de mantenimiento. Algunos cambios de los parámetros pueden causar una interrupción y se aplican en el siguiente reinicio por error.

Predeterminado: `false`

Tipo: Booleano

Obligatorio: no

AutoMinorVersionUpgrade

Este parámetro no se aplica a Amazon DocumentDB. Amazon DocumentDB no actualiza versiones secundarias, independientemente del valor establecido.

Tipo: Booleano

Obligatorio: no

CACertificateIdentifier

Indica el certificado que debe asociarse a la instancia.

Tipo: cadena

Requerido: no

CertificateRotationRestart

Especifica si la instancia de base de datos se reinicia cuando el usuario rota el certificado SSL/TLS.

Por defecto, la instancia de base de datos se reinicia cuando usted rota su certificado SSL/TLS. El certificado no se actualiza hasta que se reinicia la instancia de base de datos.

> **Important**
>
> Establezca este parámetro solo si no utiliza SSL/TLS para conectarse a la instancia de base de datos.

Si utiliza SSL/TLS para conectarse a la instancia de base de datos, consulte Cómo actualizar sus certificados de Amazon DocumentDB TLS y Cómo cifrar datos en tránsito en la Guía para desarrolladores de Amazon DocumentDB.

Tipo: Booleano

Obligatorio: no

CopyTagsToSnapshot

Es un valor que indica si se deben copiar todas las etiquetas de la instancia de base de datos en instantáneas de la instancia de base de datos. Las etiquetas no se copian de forma predeterminada.

Tipo: Booleano

Obligatorio: no

DBInstanceClass

La nueva capacidad de memoria e informática de la instancia (por ejemplo, `db.r5.large`). No todas las clases de instancia están disponibles en todas las Regiones de AWS.

Si modifica la clase de la instancia se produce una interrupción durante el cambio. El cambio se aplica durante la siguiente ventana de mantenimiento, a menos que `ApplyImmediately` se especifique como `true` para esta solicitud.

Valor predeterminado: utiliza la configuración existente.

Tipo: cadena

Requerido: no

EnablePerformanceInsights

Un valor que indica si se habilita Información sobre rendimiento para la instancia de base de datos. Para obtener más información, consulte Uso de Información sobre rendimiento de Amazon.

Tipo: Booleano

Obligatorio: no

NewDBInstanceIdentifier

El nuevo identificador de instancia para la instancia cuando se cambia el nombre de una instancia. Al cambiar el identificador de la instancia, la instancia se reiniciará inmediatamente si `Apply Immediately` se configura en `true`. Se produce durante el siguiente periodo de mantenimiento si `Apply Immediately` se configura en `false`. Este valor se almacena como una cadena en minúsculas.

Restricciones:

- Deben contener de 1 a 63 caracteres (letras, números o guiones).
- El primer carácter debe ser una letra.
- No puede terminar por un guion ni contener dos guiones consecutivos.

Ejemplo:: `mydbinstance`

Tipo: cadena

Requerido: no

PerformanceInsightsKMSKeyId

El identificador de la clave de AWS KMS para el cifrado de datos de Performance Insights.

El identificador de la clave de AWS KMS es el ARN de la clave, el identificador de clave, el ARN de alias o el nombre de alias de la clave de KMS.

Si no especifica un valor para PerformanceInsightsKMSKeyId, Amazon DocumentDB utilizará su clave KMS predeterminada. Existe una clave KMS predeterminada para su cuenta de Amazon Web Services. La cuenta de Amazon Web Services tiene una clave de KMS predeterminada diferente para cada región de Amazon Web Services.

Tipo: cadena

Requerido: no

PreferredMaintenanceWindow

El intervalo de tiempo semanal (en UTC) durante el cual puede llevarse a cabo el mantenimiento del sistema, que puede producir una interrupción. El cambio de este parámetro no produce una interrupción, salvo en la siguiente situación, y el cambio se aplica de forma asíncrona tan pronto como sea posible. Si hay acciones pendientes que provocan un reinicio, y el periodo de mantenimiento se cambia para incluir la hora actual, cambiar este parámetro provoca un reinicio de la instancia. Si traslada esta ventana a la hora actual, debe haber al menos 30 minutos entre la hora actual y el final de la ventana para garantizar que se apliquen los cambios pendientes.

Valor predeterminado: utiliza la configuración existente.

Formato: `ddd:hh24:mi-ddd:hh24:mi`

Días válidos: lunes, martes, miércoles, jueves, viernes, sábado, domingo

Restricciones: debe durar al menos 30 minutos.

Tipo: cadena

Requerido: no

PromotionTier

Valor que especifica el orden en el que se promueve una réplica de Amazon DocumentDB a la instancia primaria tras un fallo de la instancia primaria existente.

Valor predeterminado: 1

Valores válidos: 0-15

Tipo: entero

Obligatorio: no

Elementos de respuesta

El servicio devuelve el siguiente elemento.

DBInstance

Información detallada sobre una instancia.

Tipo: objeto DBInstance

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

AuthorizationNotFound

La IP CIDR o el grupo de seguridad de Amazon EC2 especificados no están autorizados para el grupo de seguridad especificado.

Es posible que Amazon DocumentDB tampoco esté autorizado para realizar las acciones necesarias en su nombre mediante IAM.

Código de estado HTTP: 404

CertificateNotFound

`CertificateIdentifier` no hace referencia a un certificado existente.

Código de estado HTTP: 404

DBInstanceAlreadyExists

Ya tiene una instancia con el identificador dado.

Código de estado HTTP: 400

DBInstanceNotFound

`DBInstanceIdentifier` no hace referencia a una instancia existente.

Código de estado HTTP: 404

DBParameterGroupNotFound

`DBParameterGroupName` no hace referencia a un grupo de parámetros existente.

Código de estado HTTP: 404

DBSecurityGroupNotFound

`DBSecurityGroupName` no hace referencia a un grupo de seguridad existente.

Código de estado HTTP: 404

DBUpgradeDependencyFailure

La actualización falló porque un recurso del que depende no puede ser modificado.

Código de estado HTTP: 400

InsufficientDBInstanceCapacity

La clase de instancia especificada no está disponible en la zona de disponibilidad especificada.

Código de estado HTTP: 400

InvalidDBInstanceState

La instancia especificada no se encuentra en el estado disponible.

Código de estado HTTP: 400

InvalidDBSecurityGroupState

El estado del grupo de seguridad no permite la eliminación.

Código de estado HTTP: 400

InvalidVPCNetworkStateFault

El grupo de subredes no cubre todas las zonas de disponibilidad después de crearla, debido a los cambios realizados.

Código de estado HTTP: 400

StorageQuotaExceeded

La solicitud provocaría que superara la cantidad permitida de almacenamiento disponible en todas las instancias.

Código de estado HTTP: 400

StorageTypeNotSupported

El almacenamiento del `StorageType` especificado no puede asociarse a la instancia de base de datos.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

ModifyDBSubnetGroup

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Modifica un grupo de subredes existente. Los grupos de subredes deben contener al menos una subred en al menos dos Zonas de Disponibilidad en la Región de AWS.

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

DBSubnetGroupName

El nombre del grupo de subredes. Este valor se almacena como una cadena en minúsculas. El grupo de subred predeterminado no se puede modificar.

Limitaciones: debe coincidir con el nombre de un existente `DBSubnetGroup`. No debe ser predeterminado.

Ejemplo:: `mySubnetgroup`

Tipo: cadena

Obligatorio: sí

SubnetIds.SubnetIdentifier.N

Los ID de subred de Amazon EC2 para el grupo de subredes.

Tipo: matriz de cadenas

Obligatorio: sí

DBSubnetGroupDescription

La descripción del grupo de subredes.

Tipo: cadena

Requerido: no

Elementos de respuesta

El servicio devuelve el siguiente elemento.

DBSubnetGroup

Información detallada sobre un grupo de subredes.

Tipo: objeto DBSubnetGroup

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

DBSubnetGroupDoesNotCoverEnoughAZs

Las subredes del grupo de subredes deben incluir al menos dos zonas de disponibilidad a menos que solo haya una zona de disponibilidad.

Código de estado HTTP: 400

DBSubnetGroupNotFoundFault

`DBSubnetGroupName` no hace referencia a un grupo de subredes existente.

Código de estado HTTP: 404

DBSubnetQuotaExceededFault

La solicitud le haría exceder el número permitido de subredes en un grupo de subredes.

Código de estado HTTP: 400

InvalidSubnet

La subred solicitada no es válida o se solicitaron varias subredes que no están en la misma nube privada virtual (VPC).

Código de estado HTTP: 400

SubnetAlreadyInUse

La subred ya está en uso en la zona de disponibilidad.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

ModifyEventSubscription

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Modifica una suscripción existente de notificación de eventos de Amazon DocumentDB.

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

SubscriptionName

El nombre de la suscripción de notificación de eventos de Amazon DocumentDB.

Tipo: cadena

Obligatorio: sí

Enabled

Un valor booleano; establecida en true `true` para activar la suscripción.

Tipo: Booleano

Obligatorio: no

EventCategories.EventCategory.N

Una lista de las categorías de eventos para un `SourceType` a los que desea suscribirse.

Tipo: matriz de cadenas

Obligatorio: no

SnsTopicArn

El Nombre de recurso de Amazon (ARN) del tema SNS creado para la notificación de eventos. El ARN es creado por Amazon SNS al crear un tema y suscribirse a él.

Tipo: cadena

Requerido: no

SourceType

El tipo de origen que está generando los eventos. Por ejemplo, si desea recibir una notificación de eventos generados por una instancia, defina este parámetro como `db-instance`. Si no se especifica este valor, se devuelven todos los eventos.

Valores válidos: `db-instance`, `db-parameter-group`, `db-security-group`

Tipo: cadena

Requerido: no

Elementos de respuesta

El servicio devuelve el siguiente elemento.

EventSubscription

Información detallada sobre un evento al que se ha suscrito.

Tipo: objeto EventSubscription

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

EventSubscriptionQuotaExceeded

Ha alcanzado el número máximo de suscripciones a eventos.

Código de estado HTTP: 400

SNSInvalidTopic

Amazon SNS ha respondido que hay un problema con el tema especificado.

Código de estado HTTP: 400

SNSNoAuthorization

No tiene permiso para publicar en el tema SNS Nombre de recurso de Amazon (ARN).

Código de estado HTTP: 400

SNSTopicArnNotFound

El nombre de recurso de Amazon (ARN) del tema de SNS no existe.

Código de estado HTTP: 404

SubscriptionCategoryNotFound

La categoría proporcionada no existe.

Código de estado HTTP: 404

SubscriptionNotFound

El nombre de la suscripción no existe.

Código de estado HTTP: 404

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

ModifyGlobalCluster

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Modifica una configuración para un clúster global de Amazon DocumentDB. Puede cambiar uno o más parámetros de configuración (por ejemplo, la protección contra la eliminación) o el identificador del clúster global especificando estos parámetros y los nuevos valores de la solicitud.

> **Note**
>
> Esta acción solo se aplica a los clústeres de Amazon DocumentDB.

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

GlobalClusterIdentifier

El identificador del clúster que se va a modificar. Este parámetro no distingue entre mayúsculas y minúsculas.

Restricciones:

- Debe coincidir con el identificador de un clúster existente.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 255 caracteres.

Patrón: `[A-Za-z][0-9A-Za-z-:._]*`

Obligatorio: sí

DeletionProtection

Indica si el clúster global tiene habilitada la protección contra eliminación. El clúster global no se puede eliminar cuando está habilitada la protección contra eliminación.

Tipo: Booleano

Obligatorio: no

NewGlobalClusterIdentifier

El nuevo identificador de un clúster global al modificar un clúster global. Este valor se almacena como una cadena en minúsculas.

- Deben contener de 1 a 63 caracteres (letras, números o guiones).

  El primer carácter debe ser una letra

  No se pueden incluir dos guiones consecutivos ni acabar con guion.

Ejemplo:: `my-cluster2`

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 255 caracteres.

Patrón: `[A-Za-z][0-9A-Za-z-:._]*`

Obligatorio: no

Elementos de respuesta

El servicio devuelve el siguiente elemento.

GlobalCluster

Tipo de datos que representa un clúster global de Amazon DocumentDB.

Tipo: objeto GlobalCluster

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

GlobalClusterNotFoundFault

`GlobalClusterIdentifier` no hace referencia a un clúster global existente.

Código de estado HTTP: 404

InvalidGlobalClusterStateFault

La operación solicitada no se puede realizar mientras el clúster esté en este estado.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

RebootDBInstance

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Es posible que necesite reiniciar su instancia, normalmente por razones de mantenimiento. Por ejemplo, si realiza determinados cambios o si modifica el grupo de parámetros de clúster asociado a la instancia, deberá reiniciar la instancia para que los cambios surtan efecto.

Cuando se reinicia una instancia, se reinicia el servicio del motor de base de datos. Al reiniciar una instancia, se produce una interrupción momentánea, durante la cual su estado se establece en rebooting.

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

DBInstanceIdentifier

El identificador de instancias. Este parámetro se almacena como una cadena en minúsculas.

Restricciones:

- Debe coincidir con el identificador de un existente `DBInstance`.

Tipo: cadena

Obligatorio: sí

ForceFailover

Cuando `true`, el reinicio se realiza a través de una conmutación por error Multi-AZ.

Restricción no se puede especificar `true` si la instancia no se ha configurado para Multi-AZ.

Tipo: Booleano

Obligatorio: no

Elementos de respuesta

El servicio devuelve el siguiente elemento.

DBInstance

Información detallada sobre una instancia.

Tipo: objeto DBInstance

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

DBInstanceNotFound

`DBInstanceIdentifier` no hace referencia a una instancia existente.

Código de estado HTTP: 404

InvalidDBInstanceState

La instancia especificada no se encuentra en el estado disponible.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

RemoveFromGlobalCluster

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Separa un clúster secundario de Amazon DocumentDB de un clúster global. El clúster se convierte en un clúster independiente con capacidad de lectura y escritura en lugar de ser de solo lectura y recibir datos de un clúster principal ubicado en una región diferente.

> **Note**
>
> Esta acción solo se aplica a los clústeres de Amazon DocumentDB.

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

DbClusterIdentifier

El Nombre de recurso de Amazon (ARN) que identifica el clúster separado del clúster global de Amazon DocumentDB.

Tipo: cadena

Obligatorio: sí

GlobalClusterIdentifier

El identificador de clúster que se va a separar del clúster global de Amazon DocumentDB.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 255 caracteres.

Patrón: `[A-Za-z][0-9A-Za-z-:._]*`

Obligatorio: sí

Elementos de respuesta

El servicio devuelve el siguiente elemento.

GlobalCluster

Tipo de datos que representa un clúster global de Amazon DocumentDB.

Tipo: objeto GlobalCluster

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

DBClusterNotFoundFault

`DBClusterIdentifier` no hace referencia a un clúster existente.

Código de estado HTTP: 404

GlobalClusterNotFoundFault

`GlobalClusterIdentifier` no hace referencia a un clúster global existente.

Código de estado HTTP: 404

InvalidGlobalClusterStateFault

La operación solicitada no se puede realizar mientras el clúster esté en este estado.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- SDK de AWS para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin

- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK de para Ruby V3

RemoveSourceIdentifierFromSubscription

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Elimina un identificador de origen de una suscripción a notificaciones de eventos de Amazon DocumentDB existente.

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

SourceIdentifier

El identificador de origen que se va a eliminar de la suscripción, por ejemplo, el identificador de instancias para una instancia o el nombre de un grupo de seguridad.

Tipo: cadena

Obligatorio: sí

SubscriptionName

El nombre de la suscripción a notificaciones de eventos de Amazon DocumentDB del que desea eliminar un identificador de origen.

Tipo: cadena

Obligatorio: sí

Elementos de respuesta

El servicio devuelve el siguiente elemento.

EventSubscription

Información detallada sobre un evento al que se ha suscrito.

Tipo: objeto EventSubscription

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

SourceNotFound

No se ha encontrado el origen solicitado.

Código de estado HTTP: 404

SubscriptionNotFound

El nombre de la suscripción no existe.

Código de estado HTTP: 404

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- SDK de AWS para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK de para Ruby V3

RemoveTagsFromResource

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Elimina las etiquetas de metadatos de un recurso de Amazon DocumentDB.

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

ResourceName

El recurso de Amazon DocumentDB del que se eliminan las etiquetas. Este valor es un Nombre de recurso de Amazon (ARN).

Tipo: cadena

Obligatorio: sí

TagKeys.member.N

La clave de la etiqueta (nombre) de la etiqueta que se va a eliminar.

Tipo: matriz de cadenas

Obligatorio: sí

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

DBClusterNotFoundFault

`DBClusterIdentifier` no hace referencia a un clúster existente.

Código de estado HTTP: 404

DBInstanceNotFound

`DBInstanceIdentifier` no hace referencia a una instancia existente.

Código de estado HTTP: 404

DBSnapshotNotFound

`DBSnapshotIdentifier` no hace referencia a una instantánea existente.

Código de estado HTTP: 404

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

ResetDBClusterParameterGroup

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Modifica los parámetros de un grupo de parámetros de clúster al valor predeterminado. Para restablecer parámetros específicos, envíe una lista de lo siguiente: `ParameterName` y `ApplyMethod`. Para restablecer el grupo de parámetros de clúster completo, especifique los parámetros de `DBClusterParameterGroupName` y `ResetAllParameters`.

Cuando restablece todo el grupo, los parámetros dinámicos se actualizan de forma inmediata y los parámetros estáticos se establecen en `pending-reboot` para su aplicación la próxima vez que se reinicie la instancia de base de datos.

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

DBClusterParameterGroupName

El nombre del grupo de parámetros de clúster que se va a restablecer.

Tipo: cadena

Obligatorio: sí

Parameters.Parameter.N

Una lista de nombres de parámetros en el grupo de parámetros de clúster que se va a restablecer a los valores predeterminados. No puede utilizar este parámetro si el parámetro `ResetAllParameters` está establecido en `true`.

Tipo: matriz de objetos Parameter

Obligatorio: no

ResetAllParameters

Un valor que se establece en `true` para restablecer todos los parámetros en el grupo de parámetros de clúster a sus valores predeterminados, y en `false` en caso contrario. No puede utilizar este parámetro si hay una lista de nombres de parámetros especificados para el parámetro `Parameters`.

Tipo: Booleano

Obligatorio: no

Elementos de respuesta

El servicio devuelve el siguiente elemento.

DBClusterParameterGroupName

El nombre del grupo de parámetros de clúster.

Restricciones:

- Debe tener de 1 a 255 letras o números.
- El primer carácter debe ser una letra.
- No puede terminar por un guion ni contener dos guiones consecutivos.

> **Note**
>
> Este valor se almacena como una cadena en minúsculas.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

DBParameterGroupNotFound

`DBParameterGroupName` no hace referencia a un grupo de parámetros existente.

Código de estado HTTP: 404

InvalidDBParameterGroupState

El grupo de parámetros está en uso o se encuentra en un estado que no es válido. Si intenta eliminar el grupo de parámetros, no puede eliminarlo cuando el grupo de parámetros se encuentra en este estado.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

RestoreDBClusterFromSnapshot

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Crea un nuevo clúster desde una instantánea o una instantánea del clúster.

Si se especifica una instantánea, el clúster de destino se crea a partir de la instantánea de base de datos de origen con una configuración predeterminada y grupo de seguridad predeterminado.

Si se especifica una instantánea del clúster, el clúster de destino se crea a partir del clúster de origen con la misma configuración que el clúster de base de datos de origen original, salvo que el nuevo clúster se crea con el grupo de seguridad predeterminado.

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

DBClusterIdentifier

El nombre del clúster que se va a crear a partir de la instantánea o de la instantánea del clúster. Este parámetro no distingue entre mayúsculas y minúsculas.

Restricciones:

- Deben contener de 1 a 63 caracteres (letras, números o guiones).
- El primer carácter debe ser una letra.
- No puede terminar por un guion ni contener dos guiones consecutivos.

Ejemplo:: `my-snapshot-id`

Tipo: cadena

Obligatorio: sí

Engine

Motor que se va a usar para el clúster nuevo.

Predeterminado: igual que el de origen.

Restricción: debe ser compatible con el motor del origen.

Tipo: cadena

Obligatorio: sí

SnapshotIdentifier

Identificador de la instantánea o instantánea del clúster desde la que se debe realizar la restauración.

Puede utilizar el nombre o el Nombre de recurso de Amazon (ARN) para especificar una instantánea del clúster. Sin embargo, puede utilizar únicamente el ARN para especificar una instantánea.

Restricciones:

- Debe coincidir con el identificador de una instantánea existente.

Tipo: cadena

Obligatorio: sí

AvailabilityZones.AvailabilityZone.N

Proporciona la lista de zonas de disponibilidad de Amazon EC2 donde se pueden crear las instancias del clúster de base de datos.

Tipo: matriz de cadenas

Obligatorio: no

DBClusterParameterGroupName

El nombre del grupo de parámetros del clúster de base de datos que desea asociar a este clúster de base de datos.

Tipo: cadena. Obligatorio: no

Si se omite este argumento, se utiliza el grupo de parámetros de clúster de base de datos predeterminado. Si se suministra, debe coincidir con el nombre de un grupo de parámetros de clúster de base de datos predeterminado existente. La cadena debe contener de 1 a 255 caracteres, letras, números o guiones. El primer carácter debe ser una letra y no puede terminar con un guion o contener dos guiones seguidos.

Tipo: cadena

Requerido: no

DBSubnetGroupName

El nombre del grupo de subredes que se va a usar para el clúster nuevo.

Limitaciones: si se suministra, debe coincidir con el nombre de un `DBSubnetGroup` existente.

Ejemplo:: `mySubnetgroup`

Tipo: cadena

Requerido: no

DeletionProtection

Especifica si se puede eliminar este clúster. Si `DeletionProtection` está habilitado, no se puede eliminar el clúster a menos que se modifique y `DeletionProtection` esté deshabilitado. `DeletionProtection` protege los clústeres de una eliminación accidental.

Tipo: Booleano

Obligatorio: no

EnableCloudwatchLogsExports.member.N

La lista de tipos de registro que deben habilitarse para exportar a los registros de Amazon CloudWatch.

Tipo: matriz de cadenas

Obligatorio: no

EngineVersion

La versión del motor que se va a usar para el clúster nuevo.

Tipo: cadena

Requerido: no

KmsKeyId

El identificador de la clave de AWS KMS que se utiliza para restaurar un clúster cifrado a partir de una instantánea o un clúster.

El identificador de la clave de AWS KMS es el nombre de recurso de Amazon (ARN) de la clave de cifrado de AWS KMS. Si está restaurando un clúster con la misma Cuenta de AWS a la que

pertenece la clave de cifrado de AWS KMS utilizada para cifrar el clúster nuevo, puede utilizar el alias de la clave de AWS KMS en lugar del ARN para la clave de cifrado de AWS KMS.

Si no se especifica un valor para el parámetro `KmsKeyId`, ocurre lo siguiente:

- Si se cifra la instantánea o la instantánea de clúster en `SnapshotIdentifier`, se cifra el clúster restaurado con la clave de AWS KMS que se utilizó para cifrar la instantánea o el clúster.
- Si la instantánea o el clúster de `SnapshotIdentifier` no está cifrada, el clúster de base de datos restaurado no está cifrado.

Tipo: cadena

Requerido: no

NetworkType

El tipo de red del clúster.

El tipo de red viene determinado por el `DBSubnetGroup` especificado para el clúster. Un `DBSubnetGroup` admite solamente el protocolo IPv4 o los protocolos IPv4 e IPv6 (`DUAL`).

Para obtener más información, consulte Clústeres de DocumentDB en una VPC en la Guía para desarrolladores de Amazon DocumentDB.

Valores válidos: `IPV4` | `DUAL`

Tipo: cadena

Requerido: no

Port

El número de puerto en el que el nuevo clúster acepta las conexiones.

Restricciones: el valor debe estar entre `1150` y `65535`.

Valor predeterminado: el mismo puerto que el clúster original.

Tipo: entero

Obligatorio: no

ServerlessV2ScalingConfiguration

Contiene la configuración de escalado de un clúster de Amazon DocumentDB sin servidor.

Tipo: objeto ServerlessV2ScalingConfiguration

Obligatorio: no

StorageType

El tipo de almacenamiento que se va a asociar al clúster de base de datos.

Para obtener información sobre los tipos de almacenamiento de los clústeres de Amazon DocumentDB, consulte Cluster storage configurations en la Guía para desarrolladores de Amazon DocumentDB.

Valores válidos para el tipo de almacenamiento: `standard | iopt1`

El valor predeterminado es `standard`

Tipo: cadena

Requerido: no

Tags.Tag.N

Las etiquetas que se van a asignar al clúster restaurado.

Tipo: matriz de objetos Tag

Obligatorio: no

VpcSecurityGroupIds.VpcSecurityGroupId.N

Una lista de grupos de seguridad de la nube privada virtual (VPC) a la que pertenecerá el nuevo clúster.

Tipo: matriz de cadenas

Obligatorio: no

Elementos de respuesta

El servicio devuelve el siguiente elemento.

DBCluster

Información detallada sobre un clúster.

Tipo: objeto DBCluster

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

DBClusterAlreadyExistsFault

El usuario ya tiene un clúster con el identificador concreto.

Código de estado HTTP: 400

DBClusterQuotaExceededFault

No se puede crear el clúster porque ha alcanzado la cuota de clústeres máxima permitida.

Código de estado HTTP: 403

DBClusterSnapshotNotFoundFault

`DBClusterSnapshotIdentifier` no hace referencia a una instantánea de un clúster existente.

Código de estado HTTP: 404

DBSnapshotNotFound

`DBSnapshotIdentifier` no hace referencia a una instantánea existente.

Código de estado HTTP: 404

DBSubnetGroupNotFoundFault

`DBSubnetGroupName` no hace referencia a un grupo de subredes existente.

Código de estado HTTP: 404

DBSubnetGroupNotFoundFault

`DBSubnetGroupName` no hace referencia a un grupo de subredes existente.

Código de estado HTTP: 404

InsufficientDBClusterCapacityFault

El clúster no tiene capacidad suficiente para la operación actual.

Código de estado HTTP: 403

InsufficientStorageClusterCapacity

No hay bastante almacenamiento disponible para la acción en curso. Es posible que pueda resolver este error mediante la actualización de su grupo de subredes para utilizar diferentes zonas de disponibilidad que tienen más almacenamiento disponible.

Código de estado HTTP: 400

InvalidDBClusterSnapshotStateFault

El valor proporcionado no es un estado de instantánea de clúster válido.

Código de estado HTTP: 400

InvalidDBSnapshotState

El estado de la instantánea no permite la eliminación.

Código de estado HTTP: 400

InvalidRestoreFault

No puede restaurar desde una copia de seguridad de una nube privada virtual (VPC) a una instancia de base de datos que no sea de VPC.

Código de estado HTTP: 400

InvalidSubnet

La subred solicitada no es válida o se solicitaron varias subredes que no están en la misma nube privada virtual (VPC).

Código de estado HTTP: 400

InvalidVPCNetworkStateFault

El grupo de subredes no cubre todas las zonas de disponibilidad después de crearla, debido a los cambios realizados.

Código de estado HTTP: 400

KMSKeyNotAccessibleFault

Se ha producido un error al acceder a una clave de AWS KMS.

Código de estado HTTP: 400

NetworkTypeNotSupported

El tipo de red no es compatible con `DBSubnetGroup` ni con la versión del motor de base de datos.

Código de estado HTTP: 400

StorageQuotaExceeded

La solicitud provocaría que superara la cantidad permitida de almacenamiento disponible en todas las instancias.

Código de estado HTTP: 400

StorageQuotaExceeded

La solicitud provocaría que superara la cantidad permitida de almacenamiento disponible en todas las instancias.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

RestoreDBClusterToPointInTime

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Restaura un clúster a un punto arbitrario en el tiempo. Los usuarios pueden restaurar a cualquier punto en el tiempo antes de `LatestRestorableTime` durante un máximo de `BackupRetentionPeriod` días. El clúster de destino se crea a partir del clúster de base de datos de origen con la misma configuración que el clúster original, salvo que el nuevo clúster se crea con el grupo de seguridad predeterminado.

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

DBClusterIdentifier

El nombre del nuevo clúster que se va a crear.

Restricciones:

- Deben contener de 1 a 63 caracteres (letras, números o guiones).
- El primer carácter debe ser una letra.
- No puede terminar por un guion ni contener dos guiones consecutivos.

Tipo: cadena

Obligatorio: sí

SourceDBClusterIdentifier

El identificador del clúster de origen desde el que se va a restaurar.

Restricciones:

- Debe coincidir con el identificador de un `DBCluster` existente.

Tipo: cadena

Obligatorio: sí

DBSubnetGroupName

El nombre del grupo de subredes que se va a usar para el clúster nuevo.

Limitaciones: si se suministra, debe coincidir con el nombre de un `DBSubnetGroup` existente.

Ejemplo:: `mySubnetgroup`

Tipo: cadena

Requerido: no

DeletionProtection

Especifica si se puede eliminar este clúster. Si `DeletionProtection` está habilitado, no se puede eliminar el clúster a menos que se modifique y `DeletionProtection` esté deshabilitado. `DeletionProtection` protege los clústeres de una eliminación accidental.

Tipo: Booleano

Obligatorio: no

EnableCloudwatchLogsExports.member.N

La lista de tipos de registro que deben habilitarse para exportar a los registros de Amazon CloudWatch.

Tipo: matriz de cadenas

Obligatorio: no

KmsKeyId

El identificador de la clave de AWS KMS que se utiliza para restaurar un clúster cifrado a partir de un clúster cifrado.

El identificador de la clave de AWS KMS es el nombre de recurso de Amazon (ARN) de la clave de cifrado de AWS KMS. Si está restaurando un clúster con la misma Cuenta de AWS a la que pertenece la clave de cifrado de AWS KMS utilizada para cifrar el clúster nuevo, puede utilizar el alias de la clave de AWS KMS en lugar del ARN para la clave de cifrado de AWS KMS.

Puede restaurar a un nuevo clúster y cifrar el nuevo clúster con una clave de AWS KMS que es diferente de la clave de AWS KMS utilizada para cifrar el clúster de origen. El nuevo clúster de base de datos se cifra con la clave de AWS KMS identificada por el parámetro `KmsKeyId`.

Si no se especifica un valor para el parámetro `KmsKeyId`, ocurre lo siguiente:

- Si el clúster está cifrado, el clúster restaurado se cifra usando la clave de AWS KMS que se usó para cifrar el clúster de origen.
- Si el clúster no está cifrado, el clúster restaurado no estará cifrado.

Si `DBClusterIdentifier` se refiere a un clúster que no está cifrado, se rechaza la solicitud de restauración.

Tipo: cadena

Requerido: no

NetworkType

El tipo de red del clúster.

El tipo de red viene determinado por el `DBSubnetGroup` especificado para el clúster. Un `DBSubnetGroup` admite solamente el protocolo IPv4 o los protocolos IPv4 e IPv6 (`DUAL`).

Para obtener más información, consulte Clústeres de DocumentDB en una VPC en la Guía para desarrolladores de Amazon DocumentDB.

Valores válidos: `IPV4` | `DUAL`

Tipo: cadena

Requerido: no

Port

El número de puerto en el que el nuevo clúster acepta las conexiones.

Restricciones: el valor debe estar entre `1150` y `65535`.

Predeterminado: el puerto predeterminado para el motor.

Tipo: entero

Obligatorio: no

RestoreToTime

La fecha y la hora a la que se va a restaurar el clúster.

Valores válidos: una hora en formato de tiempo universal coordinado (UTC).

Restricciones:

- Debe ser anterior a la última hora restaurable de la instancia.
- Debe especificarse si no se proporciona el parámetro `UseLatestRestorableTime`.

- No se puede especificar si el parámetro `UseLatestRestorableTime` es `true`.
- No se puede especificar si el parámetro `RestoreType` es `copy-on-write`.

Ejemplo:: `2015-03-07T23:45:00Z`

Tipo: marca temporal

Obligatorio: no

RestoreType

El tipo de restauración que se va a realizar. Puede especificar uno de los siguientes valores:

- `full-copy`: el nuevo clúster de base de datos se restaura como una copia completa del clúster de la base de datos de origen.
- `copy-on-write`: el nuevo clúster de base de datos se restaura como un clon del clúster de la base de datos de origen.

Restricciones: no puede especificar `copy-on-write` si la versión del motor del clúster de base de datos de origen es anterior a la 1.11.

Si no especifica un valor `RestoreType`, el nuevo clúster de base de datos se restaura como una copia completa del clúster de la base de datos de origen.

Tipo: cadena

Requerido: no

ServerlessV2ScalingConfiguration

Contiene la configuración de escalado de un clúster de Amazon DocumentDB sin servidor.

Tipo: objeto ServerlessV2ScalingConfiguration

Obligatorio: no

StorageType

El tipo de almacenamiento que se va a asociar al clúster de base de datos.

Para obtener información sobre los tipos de almacenamiento de los clústeres de Amazon DocumentDB, consulte Cluster storage configurations en la Guía para desarrolladores de Amazon DocumentDB.

Valores válidos para el tipo de almacenamiento: `standard | iopt1`

El valor predeterminado es `standard`

Tipo: cadena

Requerido: no

Tags.Tag.N

Las etiquetas que se van a asignar al clúster restaurado.

Tipo: matriz de objetos Tag

Obligatorio: no

UseLatestRestorableTime

Un valor que se establece en `true` para restaurar el clúster a la hora de la última copia de seguridad restaurable y `false` en caso contrario.

Predeterminado: `false`

Restricciones: no se puede especificar si se proporciona el parámetro `RestoreToTime`.

Tipo: Booleano

Obligatorio: no

VpcSecurityGroupIds.VpcSecurityGroupId.N

Una lista de grupos de seguridad de VPC a los que pertenece el clúster nuevo.

Tipo: matriz de cadenas

Obligatorio: no

Elementos de respuesta

El servicio devuelve el siguiente elemento.

DBCluster

Información detallada sobre un clúster.

Tipo: objeto DBCluster

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

DBClusterAlreadyExistsFault

El usuario ya tiene un clúster con el identificador concreto.

Código de estado HTTP: 400

DBClusterNotFoundFault

`DBClusterIdentifier` no hace referencia a un clúster existente.

Código de estado HTTP: 404

DBClusterQuotaExceededFault

No se puede crear el clúster porque ha alcanzado la cuota de clústeres máxima permitida.

Código de estado HTTP: 403

DBClusterSnapshotNotFoundFault

`DBClusterSnapshotIdentifier` no hace referencia a una instantánea de un clúster existente.

Código de estado HTTP: 404

DBSubnetGroupNotFoundFault

`DBSubnetGroupName` no hace referencia a un grupo de subredes existente.

Código de estado HTTP: 404

InsufficientDBClusterCapacityFault

El clúster no tiene capacidad suficiente para la operación actual.

Código de estado HTTP: 403

InsufficientStorageClusterCapacity

No hay bastante almacenamiento disponible para la acción en curso. Es posible que pueda resolver este error mediante la actualización de su grupo de subredes para utilizar diferentes zonas de disponibilidad que tienen más almacenamiento disponible.

Código de estado HTTP: 400

InvalidDBClusterSnapshotStateFault

El valor proporcionado no es un estado de instantánea de clúster válido.

Código de estado HTTP: 400

InvalidDBClusterStateFault

El clúster no se encuentra en un estado válido.

Código de estado HTTP: 400

InvalidDBSnapshotState

El estado de la instantánea no permite la eliminación.

Código de estado HTTP: 400

InvalidRestoreFault

No puede restaurar desde una copia de seguridad de una nube privada virtual (VPC) a una instancia de base de datos que no sea de VPC.

Código de estado HTTP: 400

InvalidSubnet

La subred solicitada no es válida o se solicitaron varias subredes que no están en la misma nube privada virtual (VPC).

Código de estado HTTP: 400

InvalidVPCNetworkStateFault

El grupo de subredes no cubre todas las zonas de disponibilidad después de crearla, debido a los cambios realizados.

Código de estado HTTP: 400

KMSKeyNotAccessibleFault

Se ha producido un error al acceder a una clave de AWS KMS.

Código de estado HTTP: 400

NetworkTypeNotSupported

El tipo de red no es compatible con `DBSubnetGroup` ni con la versión del motor de base de datos.

Código de estado HTTP: 400

StorageQuotaExceeded

La solicitud provocaría que superara la cantidad permitida de almacenamiento disponible en todas las instancias.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

StartDBCluster

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Reinicia el clúster detenido que está especificado por `DBClusterIdentifier`. Para obtener más información, consulte Cómo detener e iniciar un clúster de Amazon DocumentDB.

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

DBClusterIdentifier

El identificador del clúster que se va a reiniciar. Ejemplo:: `docdb-2019-05-28-15-24-52`

Tipo: cadena

Obligatorio: sí

Elementos de respuesta

El servicio devuelve el siguiente elemento.

DBCluster

Información detallada sobre un clúster.

Tipo: objeto DBCluster

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

DBClusterNotFoundFault

`DBClusterIdentifier` no hace referencia a un clúster existente.

Código de estado HTTP: 404

InvalidDBClusterStateFault

El clúster no se encuentra en un estado válido.

Código de estado HTTP: 400

InvalidDBInstanceState

La instancia especificada no se encuentra en el estado disponible.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

StopDBCluster

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Detiene el clúster en ejecución especificado por `DBClusterIdentifier`. El estado del clúster debe ser disponible. Para obtener más información, consulte Cómo detener e iniciar un clúster de Amazon DocumentDB.

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

DBClusterIdentifier

El identificador del clúster que se va a pausar. Ejemplo:: `docdb-2019-05-28-15-24-52`

Tipo: cadena

Obligatorio: sí

Elementos de respuesta

El servicio devuelve el siguiente elemento.

DBCluster

Información detallada sobre un clúster.

Tipo: objeto DBCluster

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

DBClusterNotFoundFault

`DBClusterIdentifier` no hace referencia a un clúster existente.

Código de estado HTTP: 404

InvalidDBClusterStateFault

El clúster no se encuentra en un estado válido.

Código de estado HTTP: 400

InvalidDBInstanceState

La instancia especificada no se encuentra en el estado disponible.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

SwitchoverGlobalCluster

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Cambia el clúster de Amazon DocumentDB secundario especificado para que sea el nuevo clúster de Amazon DocumentDB principal del clúster de base de datos global.

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

GlobalClusterIdentifier

El identificador del clúster de base de datos global de Amazon DocumentDB que va a hacer la transición. El identificador es la clave única asignada por el usuario cuando se creó el clúster. Dicho de otro modo, es el nombre del clúster global. Este parámetro no distingue entre mayúsculas y minúsculas.

Restricciones:

- Debe coincidir con el identificador de un clúster global existente (base de datos global de Amazon DocumentDB).
- Longitud mínima de 1. La longitud máxima es de 255 caracteres.

Patrón: `[A-Za-z][0-9A-Za-z-:._]*`

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 255 caracteres.

Patrón: `[A-Za-z][0-9A-Za-z-:._]*`

Obligatorio: sí

TargetDbClusterIdentifier

El identificador del clúster secundario de Amazon DocumentDB que desea promover para que sea el nuevo principal del clúster de base de datos global. Utilice el Nombre de recurso de Amazon (ARN) para el identificador de modo que Amazon DocumentDB pueda localizar el clúster en su región de AWS.

Restricciones:

- Debe coincidir con el identificador de un clúster secundario existente.
- Longitud mínima de 1. La longitud máxima es de 255 caracteres.

Patrón: `[A-Za-z][0-9A-Za-z-:._]*`

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 255 caracteres.

Patrón: `[A-Za-z][0-9A-Za-z-:._]*`

Obligatorio: sí

Elementos de respuesta

El servicio devuelve el siguiente elemento.

GlobalCluster

Tipo de datos que representa un clúster global de Amazon DocumentDB.

Tipo: objeto GlobalCluster

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

DBClusterNotFoundFault

`DBClusterIdentifier` no hace referencia a un clúster existente.

Código de estado HTTP: 404

GlobalClusterNotFoundFault

`GlobalClusterIdentifier` no hace referencia a un clúster global existente.

Código de estado HTTP: 404

InvalidDBClusterStateFault

El clúster no se encuentra en un estado válido.

Código de estado HTTP: 400

InvalidGlobalClusterStateFault

La operación solicitada no se puede realizar mientras el clúster esté en este estado.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

Amazon DocumentDB Elastic Clusters

Los clústeres elásticos de Amazon DocumentDB admiten las siguientes acciones:

- ApplyPendingMaintenanceAction
- CopyClusterSnapshot
- CreateCluster
- CreateClusterSnapshot
- DeleteCluster
- DeleteClusterSnapshot
- GetCluster

- GetClusterSnapshot
- GetPendingMaintenanceAction
- ListClusters
- ListClusterSnapshots
- ListPendingMaintenanceActions
- ListTagsForResource
- RestoreClusterFromSnapshot
- StartCluster
- StopCluster
- TagResource
- UntagResource
- UpdateCluster

ApplyPendingMaintenanceAction

Servicio: Amazon DocumentDB Elastic Clusters

El tipo de acción de mantenimiento pendiente que se aplica a este recurso.

Sintaxis de la solicitud

```
POST /pending-action HTTP/1.1
Content-type: application/json

{
   "applyAction": "string",
   "applyOn": "string",
   "optInType": "string",
   "resourceArn": "string"
}
```

Parámetros de solicitud del URI

La solicitud no utiliza ningún parámetro de URI.

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

applyAction

La acción de mantenimiento pendiente que se aplica a este recurso.

Las acciones válidas son:

- ENGINE_UPDATE
- ENGINE_UPGRADE
- SECURITY_UPDATE
- OS_UPDATE
- MASTER_USER_PASSWORD_UPDATE

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 256 caracteres.

Obligatorio: sí

optInType

Un valor que indica el tipo de solicitud de alta o deshace una solicitud de alta. Una solicitud de alta de tipo `IMMEDIATE` no se puede deshacer.

Tipo: cadena

Valores válidos: `IMMEDIATE | NEXT_MAINTENANCE | APPLY_ON | UNDO_OPT_IN`

Obligatorio: sí

resourceArn

El Nombre de recurso de Amazon (ARN) Amazon DocumentDB del recurso al que se aplica la acción de mantenimiento pendiente.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 256 caracteres.

Obligatorio: sí

applyOn

Una fecha específica para aplicar la acción de mantenimiento pendiente. Obligatorio si el tipo de suscripción es `APPLY_ON`. Formato: `yyyy/MM/dd HH:mm-yyyy/MM/dd HH:mm`

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 256 caracteres.

Obligatorio: no

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
   "resourcePendingMaintenanceAction": {
      "pendingMaintenanceActionDetails": [
         {
            "action": "string",
            "autoAppliedAfterDate": "string",
```

```
            "currentApplyDate": "string",
            "description": "string",
            "forcedApplyDate": "string",
            "optInStatus": "string"
         }
      ],
      "resourceArn": "string"
   }
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

resourcePendingMaintenanceAction

El resultado de la acción de mantenimiento pendiente que se aplica.

Tipo: objeto ResourcePendingMaintenanceAction

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

AccessDeniedException

Una excepción que se produce cuando no hay permisos suficientes para realizar una acción.

message

Un mensaje de error que explica por qué se denegó el acceso.

Código de estado HTTP: 403

ConflictException

Se ha producido un conflicto de acceso.

resourceId

El identificador del recurso en el que se produjo un conflicto de acceso.

resourceType

El tipo del recurso en el que se produjo un conflicto de acceso.

Código de estado HTTP: 409

InternalServerException

Se ha producido un error en el servidor interno.

Código de estado HTTP: 500

ResourceNotFoundException

No se pudo encontrar el recurso especificado.

message

Un mensaje de error que describe el error.

resourceId

El identificador del recurso que no se pudo encontrar.

resourceType

El tipo del recurso que no se pudo encontrar.

Código de estado HTTP: 404

ThrottlingException

Se lanzará ThrottlingException cuando se deniegue la solicitud debido a la limitación de la solicitud.

retryAfterSeconds

La cantidad de segundos que se debe esperar para volver a intentar la operación.

Código de estado HTTP: 429

ValidationException

Estructura que define una excepción de validación.

fieldList

Una lista de los campos en los que se produjo la excepción de validación.

message

Un mensaje de error que describe la excepción de validación.

reason

El motivo por el que se produjo la excepción de validación (uno de los siguientes: `unknownOperation`, `cannotParse`, `fieldValidationFailed` o `other`).

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

CopyClusterSnapshot

Servicio: Amazon DocumentDB Elastic Clusters

Copia una instantánea de un clúster elástico.

Sintaxis de la solicitud

```
POST /cluster-snapshot/snapshotArn/copy HTTP/1.1
Content-type: application/json

{
   "copyTags": boolean,
   "kmsKeyId": "string",
   "tags": {
      "string" : "string"
   },
   "targetSnapshotName": "string"
}
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

snapshotArn

El identificador del Nombre de recurso de Amazon (ARN) de la instantánea del clúster elástico.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

targetSnapshotName

El identificador de la nueva instantánea del clúster elástico que se va a crear a partir de la instantánea del clúster de origen. Este parámetro no distingue entre mayúsculas y minúsculas.

Restricciones:

- Deben contener de 1 a 63 caracteres (letras, números o guiones).
- El primer carácter debe ser una letra.

- No puede terminar por un guion ni contener dos guiones consecutivos.

Ejemplo:: `elastic-cluster-snapshot-5`

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 63.

Obligatorio: sí

copyTags

Establézcalo en `true` para copiar todas las etiquetas de la instantánea del clúster de origen a la instantánea del clúster de destino. El valor predeterminado es `false`.

Tipo: Booleano

Obligatorio: no

kmsKeyId

El ID de la clave de AWS KMS de una instantánea del clúster elástico cifrada. El ID de la clave de AWS KMS es el Nombre de recurso de Amazon (ARN), el identificador de la clave de AWS KMS o el alias de la clave de AWS KMS de la clave de cifrado de AWS KMS.

Si copia una instantánea del clúster elástico cifrada desde la cuenta de AWS, puede especificar un valor para `KmsKeyId` para cifrar la copia con una nueva clave de cifrado de AWS KMS. Si no especifica ningún valor para `KmsKeyId`, la copia de la instantánea del clúster elástico se cifra con la misma clave de `AWS` KMS que la instantánea del clúster elástico de origen.

Si intenta copiar una instantánea del clúster elástico sin cifrar y especificar un valor para el parámetro `KmsKeyId`, se devuelve un error.

Tipo: cadena

Requerido: no

tags

Las etiquetas que se van a asignar a la instantánea del clúster elástico.

Tipo: mapa de cadena a cadena

Limitaciones de longitud de la clave: longitud mínima de 1. Longitud máxima de 128.

Patrón de clave: `(?!aws:)[a-zA-Z+-=._:/]+`

Limitaciones de longitud de los valores: longitud mínima de 0. La longitud máxima es de 256 caracteres.

Obligatorio: no

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
   "snapshot": {
      "adminUserName": "string",
      "clusterArn": "string",
      "clusterCreationTime": "string",
      "kmsKeyId": "string",
      "snapshotArn": "string",
      "snapshotCreationTime": "string",
      "snapshotName": "string",
      "snapshotType": "string",
      "status": "string",
      "subnetIds": [ "string" ],
      "vpcSecurityGroupIds": [ "string" ]
   }
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

snapshot

Devuelve información sobre una instantánea específica del clúster elástico.

Tipo: objeto ClusterSnapshot

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

AccessDeniedException

Una excepción que se produce cuando no hay permisos suficientes para realizar una acción.

message

Un mensaje de error que explica por qué se denegó el acceso.

Código de estado HTTP: 403

ConflictException

Se ha producido un conflicto de acceso.

resourceId

El identificador del recurso en el que se produjo un conflicto de acceso.

resourceType

El tipo del recurso en el que se produjo un conflicto de acceso.

Código de estado HTTP: 409

InternalServerException

Se ha producido un error en el servidor interno.

Código de estado HTTP: 500

ResourceNotFoundException

No se pudo encontrar el recurso especificado.

message

Un mensaje de error que describe el error.

resourceId

El identificador del recurso que no se pudo encontrar.

resourceType

El tipo del recurso que no se pudo encontrar.

Código de estado HTTP: 404

ServiceQuotaExceededException

Se ha superado la cuota de servicio para la acción.

Código de estado HTTP: 402

ThrottlingException

Se lanzará ThrottlingException cuando se deniegue la solicitud debido a la limitación de la solicitud.

retryAfterSeconds

La cantidad de segundos que se debe esperar para volver a intentar la operación.

Código de estado HTTP: 429

ValidationException

Estructura que define una excepción de validación.

fieldList

Una lista de los campos en los que se produjo la excepción de validación.

message

Un mensaje de error que describe la excepción de validación.

reason

El motivo por el que se produjo la excepción de validación (uno de los siguientes: `unknownOperation`, `cannotParse`, `fieldValidationFailed` o `other`).

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3

- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

CreateCluster

Servicio: Amazon DocumentDB Elastic Clusters

Crea un nuevo clúster elástico de Amazon DocumentDB y devuelve su estructura de clúster.

Sintaxis de la solicitud

```
POST /cluster HTTP/1.1
Content-type: application/json

{
   "adminUserName": "string",
   "adminUserPassword": "string",
   "authType": "string",
   "backupRetentionPeriod": number,
   "clientToken": "string",
   "clusterName": "string",
   "kmsKeyId": "string",
   "preferredBackupWindow": "string",
   "preferredMaintenanceWindow": "string",
   "shardCapacity": number,
   "shardCount": number,
   "shardInstanceCount": number,
   "subnetIds": [ "string" ],
   "tags": {
      "string" : "string"
   },
   "vpcSecurityGroupIds": [ "string" ]
}
```

Parámetros de solicitud del URI

La solicitud no utiliza ningún parámetro de URI.

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

adminUserName

El nombre del administrador de clústeres elásticos de Amazon DocumentDB.

Restricciones:

- Debe tener de 1 a 63 letras o números.
- El primer carácter debe ser una letra.
- No puede ser una palabra reservada.

Tipo: cadena

Obligatorio: sí

adminUserPassword

La contraseña del administrador de clústeres elásticos de Amazon DocumentDB. La contraseña puede contener cualquier carácter ASCII imprimible.

Restricciones:

- Debe contener de 8 a 100 caracteres.
- No puede contener una barra inclinada (/), comillas dobles (“ ”) ni el símbolo de “arroba” (@).

Tipo: cadena

Obligatorio: sí

authType

El tipo de autenticación utilizado para determinar dónde buscar la contraseña que se usa para acceder al clúster elástico. Los tipos válidos son `PLAIN_TEXT` o `SECRET_ARN`.

Tipo: cadena

Valores válidos: `PLAIN_TEXT | SECRET_ARN`

Obligatorio: sí

clusterName

El nombre del nuevo clúster elástico. Este parámetro se almacena como una cadena en minúsculas.

Restricciones:

- Deben contener de 1 a 63 caracteres (letras, números o guiones).
- El primer carácter debe ser una letra.
- No puede terminar por un guion ni contener dos guiones consecutivos.

Ejemplo: `my-cluster`

Tipo: cadena

Obligatorio: sí

shardCapacity

La cantidad de vCPU asignadas a cada partición de clúster elástico. El máximo es 64. Los valores permitidos son 2, 4, 8, 16, 32, 64.

Tipo: número entero

Obligatorio: sí

shardCount

El número de particiones asignadas al clúster elástico. El máximo es 32.

Tipo: número entero

Obligatorio: sí

backupRetentionPeriod

El número de días durante los que se conservan las instantáneas de base de datos automáticas.

Tipo: entero

Obligatorio: no

clientToken

El token de cliente del clúster elástico.

Tipo: cadena

Requerido: no

kmsKeyId

El identificador de clave de KMS que se debe utilizar para cifrar el nuevo clúster elástico.

El identificador de la clave de KMS es el Nombre de recurso de Amazon (ARN) de la clave de cifrado de KMS. Si está creando un clúster con la misma cuenta de Amazon a la que pertenece

esta clave de cifrado de KMS, puede utilizar el alias de la clave de KMS en lugar del ARN como clave de cifrado de KMS.

Si no se especifica una clave de cifrado, Amazon DocumentDB utiliza la clave de cifrado predeterminada que KMS crea para la cuenta. Su cuenta dispone de una clave de cifrado predeterminada diferente para cada región de Amazon.

Tipo: cadena

Requerido: no

preferredBackupWindow

El intervalo de tiempo diario durante el que se crean las copias de seguridad automatizadas si las copias de seguridad automatizadas están habilitadas según lo determina `backupRetentionPeriod`.

Tipo: cadena

Requerido: no

preferredMaintenanceWindow

El intervalo de tiempo semanal durante el cual puede llevarse a cabo el mantenimiento del sistema, en tiempo universal coordinado (UTC).

Formato: `ddd:hh24:mi-ddd:hh24:mi`

El valor predeterminado es un periodo de 30 minutos seleccionado al azar de un bloque de 8 horas de tiempo para cada Región de AWS, que tiene lugar un día de la semana al azar.

Días válidos: lunes, martes, miércoles, jueves, viernes, sábado, domingo

Restricciones: plazo mínimo de 30 minutos.

Tipo: cadena

Requerido: no

shardInstanceCount

El número de instancias de réplica que se aplica a todas las particiones del clúster elástico. Un valor de `shardInstanceCount` igual a 1 significa que hay una instancia de escritura y las

instancias adicionales son réplicas que se pueden usar para llevar a cabo lecturas y mejorar la disponibilidad.

Tipo: entero

Obligatorio: no

subnetIds

ID de subredes de Amazon EC2 para el nuevo clúster elástico.

Tipo: matriz de cadenas

Obligatorio: no

tags

Las etiquetas que se van a asignar al nuevo clúster elástico.

Tipo: mapa de cadena a cadena

Limitaciones de longitud de la clave: longitud mínima de 1. Longitud máxima de 128.

Patrón de clave: `(?!aws:)[a-zA-Z+-=._:/]+`

Limitaciones de longitud de los valores: longitud mínima de 0. La longitud máxima es de 256 caracteres.

Obligatorio: no

vpcSecurityGroupIds

Una lista de grupos de seguridad EC2 VPC para asociar con el nuevo clúster elástico.

Tipo: matriz de cadenas

Obligatorio: no

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
```

```
   "cluster": {
      "adminUserName": "string",
      "authType": "string",
      "backupRetentionPeriod": number,
      "clusterArn": "string",
      "clusterEndpoint": "string",
      "clusterName": "string",
      "createTime": "string",
      "kmsKeyId": "string",
      "preferredBackupWindow": "string",
      "preferredMaintenanceWindow": "string",
      "shardCapacity": number,
      "shardCount": number,
      "shardInstanceCount": number,
      "shards": [
         {
            "createTime": "string",
            "shardId": "string",
            "status": "string"
         }
      ],
      "status": "string",
      "subnetIds": [ "string" ],
      "vpcSecurityGroupIds": [ "string" ]
   }
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

cluster

El nuevo clúster elástico que se ha creado.

Tipo: objeto Cluster

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

AccessDeniedException

Una excepción que se produce cuando no hay permisos suficientes para realizar una acción.

message

Un mensaje de error que explica por qué se denegó el acceso.

Código de estado HTTP: 403

ConflictException

Se ha producido un conflicto de acceso.

resourceId

El identificador del recurso en el que se produjo un conflicto de acceso.

resourceType

El tipo del recurso en el que se produjo un conflicto de acceso.

Código de estado HTTP: 409

InternalServerException

Se ha producido un error en el servidor interno.

Código de estado HTTP: 500

ServiceQuotaExceededException

Se ha superado la cuota de servicio para la acción.

Código de estado HTTP: 402

ThrottlingException

Se lanzará ThrottlingException cuando se deniegue la solicitud debido a la limitación de la solicitud.

retryAfterSeconds

La cantidad de segundos que se debe esperar para volver a intentar la operación.

Código de estado HTTP: 429

ValidationException

Estructura que define una excepción de validación.

fieldList

Una lista de los campos en los que se produjo la excepción de validación.

message

Un mensaje de error que describe la excepción de validación.

reason

El motivo por el que se produjo la excepción de validación (uno de los siguientes: `unknownOperation`, `cannotParse`, `fieldValidationFailed` o `other`).

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

CreateClusterSnapshot

Servicio: Amazon DocumentDB Elastic Clusters

Crea una instantánea de un clúster elástico.

Sintaxis de la solicitud

```
POST /cluster-snapshot HTTP/1.1
Content-type: application/json

{
   "clusterArn": "string",
   "snapshotName": "string",
   "tags": {
      "string" : "string"
   }
}
```

Parámetros de solicitud del URI

La solicitud no utiliza ningún parámetro de URI.

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

clusterArn

El identificador ARN del clúster elástico del que desea crear una instantánea.

Tipo: cadena

Obligatorio: sí

snapshotName

Nombre de la nueva instantánea del clúster elástico.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 63.

Obligatorio: sí

tags

Las etiquetas que se van a asignar a la instantánea del nuevo clúster elástico.

Tipo: mapa de cadena a cadena

Limitaciones de longitud de la clave: longitud mínima de 1. Longitud máxima de 128.

Patrón de clave: `(?!aws:)[a-zA-Z+-=._:/]+`

Limitaciones de longitud de los valores: longitud mínima de 0. La longitud máxima es de 256 caracteres.

Obligatorio: no

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
   "snapshot": {
      "adminUserName": "string",
      "clusterArn": "string",
      "clusterCreationTime": "string",
      "kmsKeyId": "string",
      "snapshotArn": "string",
      "snapshotCreationTime": "string",
      "snapshotName": "string",
      "snapshotType": "string",
      "status": "string",
      "subnetIds": [ "string" ],
      "vpcSecurityGroupIds": [ "string" ]
   }
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

snapshot

Devuelve información sobre la nueva instantánea del clúster elástico.

Tipo: objeto ClusterSnapshot

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

AccessDeniedException

Una excepción que se produce cuando no hay permisos suficientes para realizar una acción.

message

Un mensaje de error que explica por qué se denegó el acceso.

Código de estado HTTP: 403

ConflictException

Se ha producido un conflicto de acceso.

resourceId

El identificador del recurso en el que se produjo un conflicto de acceso.

resourceType

El tipo del recurso en el que se produjo un conflicto de acceso.

Código de estado HTTP: 409

InternalServerException

Se ha producido un error en el servidor interno.

Código de estado HTTP: 500

ResourceNotFoundException

No se pudo encontrar el recurso especificado.

message

Un mensaje de error que describe el error.

resourceId

El identificador del recurso que no se pudo encontrar.

resourceType

El tipo del recurso que no se pudo encontrar.

Código de estado HTTP: 404

ServiceQuotaExceededException

Se ha superado la cuota de servicio para la acción.

Código de estado HTTP: 402

ThrottlingException

Se lanzará ThrottlingException cuando se deniegue la solicitud debido a la limitación de la solicitud.

retryAfterSeconds

La cantidad de segundos que se debe esperar para volver a intentar la operación.

Código de estado HTTP: 429

ValidationException

Estructura que define una excepción de validación.

fieldList

Una lista de los campos en los que se produjo la excepción de validación.

message

Un mensaje de error que describe la excepción de validación.

reason

El motivo por el que se produjo la excepción de validación (uno de los siguientes: `unknownOperation`, `cannotParse`, `fieldValidationFailed` o `other`).

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

DeleteCluster

Servicio: Amazon DocumentDB Elastic Clusters

Elimine un clúster elástico.

Sintaxis de la solicitud

```
DELETE /cluster/clusterArn HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

clusterArn

El identificador ARN del clúster elástico que se va a eliminar.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
   "cluster": {
      "adminUserName": "string",
      "authType": "string",
      "backupRetentionPeriod": number,
      "clusterArn": "string",
      "clusterEndpoint": "string",
      "clusterName": "string",
      "createTime": "string",
      "kmsKeyId": "string",
      "preferredBackupWindow": "string",
      "preferredMaintenanceWindow": "string",
      "shardCapacity": number,
      "shardCount": number,
```

```
      "shardInstanceCount": number,
      "shards": [
         {
            "createTime": "string",
            "shardId": "string",
            "status": "string"
         }
      ],
      "status": "string",
      "subnetIds": [ "string" ],
      "vpcSecurityGroupIds": [ "string" ]
   }
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

cluster

Devuelve información sobre el clúster eliminado recientemente.

Tipo: objeto Cluster

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

AccessDeniedException

Una excepción que se produce cuando no hay permisos suficientes para realizar una acción.

message

Un mensaje de error que explica por qué se denegó el acceso.

Código de estado HTTP: 403

ConflictException

Se ha producido un conflicto de acceso.

resourceId

El identificador del recurso en el que se produjo un conflicto de acceso.

resourceType

El tipo del recurso en el que se produjo un conflicto de acceso.

Código de estado HTTP: 409

InternalServerException

Se ha producido un error en el servidor interno.

Código de estado HTTP: 500

ResourceNotFoundException

No se pudo encontrar el recurso especificado.

message

Un mensaje de error que describe el error.

resourceId

El identificador del recurso que no se pudo encontrar.

resourceType

El tipo del recurso que no se pudo encontrar.

Código de estado HTTP: 404

ThrottlingException

Se lanzará ThrottlingException cuando se deniegue la solicitud debido a la limitación de la solicitud.

retryAfterSeconds

La cantidad de segundos que se debe esperar para volver a intentar la operación.

Código de estado HTTP: 429

ValidationException

Estructura que define una excepción de validación.

fieldList

Una lista de los campos en los que se produjo la excepción de validación.

message

Un mensaje de error que describe la excepción de validación.

reason

El motivo por el que se produjo la excepción de validación (uno de los siguientes: `unknownOperation`, `cannotParse`, `fieldValidationFailed` o `other`).

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

DeleteClusterSnapshot

Servicio: Amazon DocumentDB Elastic Clusters

Eliminación de una instantánea de un clúster elástico.

Sintaxis de la solicitud

```
DELETE /cluster-snapshot/snapshotArn HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

snapshotArn

El identificador ARN de la instantánea del clúster elástico que se va a eliminar.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
   "snapshot": {
      "adminUserName": "string",
      "clusterArn": "string",
      "clusterCreationTime": "string",
      "kmsKeyId": "string",
      "snapshotArn": "string",
      "snapshotCreationTime": "string",
      "snapshotName": "string",
      "snapshotType": "string",
      "status": "string",
      "subnetIds": [ "string" ],
      "vpcSecurityGroupIds": [ "string" ]
   }
```

```
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

snapshot

Devuelve información sobre una instantánea del clúster elástico recién detectada.

Tipo: objeto ClusterSnapshot

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

AccessDeniedException

Una excepción que se produce cuando no hay permisos suficientes para realizar una acción.

message

Un mensaje de error que explica por qué se denegó el acceso.

Código de estado HTTP: 403

ConflictException

Se ha producido un conflicto de acceso.

resourceId

El identificador del recurso en el que se produjo un conflicto de acceso.

resourceType

El tipo del recurso en el que se produjo un conflicto de acceso.

Código de estado HTTP: 409

InternalServerException

Se ha producido un error en el servidor interno.

Código de estado HTTP: 500

ResourceNotFoundException

No se pudo encontrar el recurso especificado.

message

Un mensaje de error que describe el error.

resourceId

El identificador del recurso que no se pudo encontrar.

resourceType

El tipo del recurso que no se pudo encontrar.

Código de estado HTTP: 404

ThrottlingException

Se lanzará ThrottlingException cuando se deniegue la solicitud debido a la limitación de la solicitud.

retryAfterSeconds

La cantidad de segundos que se debe esperar para volver a intentar la operación.

Código de estado HTTP: 429

ValidationException

Estructura que define una excepción de validación.

fieldList

Una lista de los campos en los que se produjo la excepción de validación.

message

Un mensaje de error que describe la excepción de validación.

reason

El motivo por el que se produjo la excepción de validación (uno de los siguientes: `unknownOperation`, `cannotParse`, `fieldValidationFailed` o `other`).

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

GetCluster

Servicio: Amazon DocumentDB Elastic Clusters

Devuelve información sobre un clúster elástico específico.

Sintaxis de la solicitud

```
GET /cluster/clusterArn HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

clusterArn

El identificador ARN del clúster elástico.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
   "cluster": {
      "adminUserName": "string",
      "authType": "string",
      "backupRetentionPeriod": number,
      "clusterArn": "string",
      "clusterEndpoint": "string",
      "clusterName": "string",
      "createTime": "string",
      "kmsKeyId": "string",
      "preferredBackupWindow": "string",
      "preferredMaintenanceWindow": "string",
      "shardCapacity": number,
      "shardCount": number,
```

```
      "shardInstanceCount": number,
      "shards": [
         {
            "createTime": "string",
            "shardId": "string",
            "status": "string"
         }
      ],
      "status": "string",
      "subnetIds": [ "string" ],
      "vpcSecurityGroupIds": [ "string" ]
   }
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

cluster

Devuelve información sobre un clúster elástico específico.

Tipo: objeto Cluster

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

AccessDeniedException

Una excepción que se produce cuando no hay permisos suficientes para realizar una acción.

message

Un mensaje de error que explica por qué se denegó el acceso.

Código de estado HTTP: 403

InternalServerException

Se ha producido un error en el servidor interno.

Código de estado HTTP: 500

ResourceNotFoundException

No se pudo encontrar el recurso especificado.

message

Un mensaje de error que describe el error.

resourceId

El identificador del recurso que no se pudo encontrar.

resourceType

El tipo del recurso que no se pudo encontrar.

Código de estado HTTP: 404

ThrottlingException

Se lanzará ThrottlingException cuando se deniegue la solicitud debido a la limitación de la solicitud.

retryAfterSeconds

La cantidad de segundos que se debe esperar para volver a intentar la operación.

Código de estado HTTP: 429

ValidationException

Estructura que define una excepción de validación.

fieldList

Una lista de los campos en los que se produjo la excepción de validación.

message

Un mensaje de error que describe la excepción de validación.

reason

El motivo por el que se produjo la excepción de validación (uno de los siguientes: `unknownOperation`, `cannotParse`, `fieldValidationFailed` o `other`).

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

GetClusterSnapshot

Servicio: Amazon DocumentDB Elastic Clusters

Devuelve información sobre una instantánea específica del clúster elástico

Sintaxis de la solicitud

```
GET /cluster-snapshot/snapshotArn HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

snapshotArn

El identificador ARN de la instantánea del clúster elástico.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
   "snapshot": {
      "adminUserName": "string",
      "clusterArn": "string",
      "clusterCreationTime": "string",
      "kmsKeyId": "string",
      "snapshotArn": "string",
      "snapshotCreationTime": "string",
      "snapshotName": "string",
      "snapshotType": "string",
      "status": "string",
      "subnetIds": [ "string" ],
      "vpcSecurityGroupIds": [ "string" ]
   }
```

```
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

snapshot

Devuelve información sobre una instantánea específica del clúster elástico.

Tipo: objeto ClusterSnapshot

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

AccessDeniedException

Una excepción que se produce cuando no hay permisos suficientes para realizar una acción.

message

Un mensaje de error que explica por qué se denegó el acceso.

Código de estado HTTP: 403

InternalServerException

Se ha producido un error en el servidor interno.

Código de estado HTTP: 500

ResourceNotFoundException

No se pudo encontrar el recurso especificado.

message

Un mensaje de error que describe el error.

resourceId

El identificador del recurso que no se pudo encontrar.

resourceType

El tipo del recurso que no se pudo encontrar.

Código de estado HTTP: 404

ThrottlingException

Se lanzará ThrottlingException cuando se deniegue la solicitud debido a la limitación de la solicitud.

retryAfterSeconds

La cantidad de segundos que se debe esperar para volver a intentar la operación.

Código de estado HTTP: 429

ValidationException

Estructura que define una excepción de validación.

fieldList

Una lista de los campos en los que se produjo la excepción de validación.

message

Un mensaje de error que describe la excepción de validación.

reason

El motivo por el que se produjo la excepción de validación (uno de los siguientes: `unknownOperation`, `cannotParse`, `fieldValidationFailed` o `other`).

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2

- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

GetPendingMaintenanceAction

Servicio: Amazon DocumentDB Elastic Clusters

Recupera todas las acciones de mantenimiento pendientes.

Sintaxis de la solicitud

```
GET /pending-action/resourceArn HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

resourceArn

Recupera las acciones de mantenimiento pendientes para un nombre de recurso de Amazon (ARN) específico.

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 256 caracteres.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
   "resourcePendingMaintenanceAction": {
      "pendingMaintenanceActionDetails": [
         {
            "action": "string",
            "autoAppliedAfterDate": "string",
            "currentApplyDate": "string",
            "description": "string",
            "forcedApplyDate": "string",
            "optInStatus": "string"
```

```
            }
        ],
        "resourceArn": "string"
    }
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

resourcePendingMaintenanceAction

Proporciona información acerca de una acción de mantenimiento pendiente para un recurso.

Tipo: objeto ResourcePendingMaintenanceAction

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

AccessDeniedException

Una excepción que se produce cuando no hay permisos suficientes para realizar una acción.

message

Un mensaje de error que explica por qué se denegó el acceso.

Código de estado HTTP: 403

ConflictException

Se ha producido un conflicto de acceso.

resourceId

El identificador del recurso en el que se produjo un conflicto de acceso.

resourceType

El tipo del recurso en el que se produjo un conflicto de acceso.

Código de estado HTTP: 409

InternalServerException

Se ha producido un error en el servidor interno.

Código de estado HTTP: 500

ResourceNotFoundException

No se pudo encontrar el recurso especificado.

message

Un mensaje de error que describe el error.

resourceId

El identificador del recurso que no se pudo encontrar.

resourceType

El tipo del recurso que no se pudo encontrar.

Código de estado HTTP: 404

ThrottlingException

Se lanzará ThrottlingException cuando se deniegue la solicitud debido a la limitación de la solicitud.

retryAfterSeconds

La cantidad de segundos que se debe esperar para volver a intentar la operación.

Código de estado HTTP: 429

ValidationException

Estructura que define una excepción de validación.

fieldList

Una lista de los campos en los que se produjo la excepción de validación.

message

Un mensaje de error que describe la excepción de validación.

reason

El motivo por el que se produjo la excepción de validación (uno de los siguientes: `unknownOperation`, `cannotParse`, `fieldValidationFailed` o `other`).

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

ListClusters

Servicio: Amazon DocumentDB Elastic Clusters

Devuelve información sobre los clústeres elásticos de Amazon DocumentDB aprovisionados.

Sintaxis de la solicitud

```
GET /clusters?maxResults=maxResults&nextToken=nextToken HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

maxResults

El número máximo de resultados de instantáneas de clúster elástico que se reciben en la respuesta.

Rango válido: valor mínimo de 1. Valor máximo de 100.

nextToken

Un token de paginación proporcionado por una solicitud anterior. Si se especifica este parámetro, la respuesta solo incluye registros más allá del token, hasta el valor especificado por `max-results`.

Si no hay más datos en la respuesta, no se devolverá el `nextToken`.

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
   "clusters": [
      {
         "clusterArn": "string",
```

```
            "clusterName": "string",
            "status": "string"
        }
    ],
    "nextToken": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

clusters

Lista de clústeres elásticos de Amazon DocumentDB.

Tipo: matriz de objetos ClusterInList

nextToken

Un token de paginación proporcionado por una solicitud anterior. Si se especifica este parámetro, la respuesta solo incluye registros más allá del token, hasta el valor especificado por `max-results`.

Si no hay más datos en la respuesta, no se devolverá el `nextToken`.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

AccessDeniedException

Una excepción que se produce cuando no hay permisos suficientes para realizar una acción.

message

Un mensaje de error que explica por qué se denegó el acceso.

Código de estado HTTP: 403

InternalServerException

Se ha producido un error en el servidor interno.

Código de estado HTTP: 500

ThrottlingException

Se lanzará ThrottlingException cuando se deniegue la solicitud debido a la limitación de la solicitud.

retryAfterSeconds

La cantidad de segundos que se debe esperar para volver a intentar la operación.

Código de estado HTTP: 429

ValidationException

Estructura que define una excepción de validación.

fieldList

Una lista de los campos en los que se produjo la excepción de validación.

message

Un mensaje de error que describe la excepción de validación.

reason

El motivo por el que se produjo la excepción de validación (uno de los siguientes: `unknownOperation`, `cannotParse`, `fieldValidationFailed` o `other`).

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2

- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

ListClusterSnapshots

Servicio: Amazon DocumentDB Elastic Clusters

Devuelve información sobre las instantáneas de un clúster elástico especificado.

Sintaxis de la solicitud

```
GET /cluster-snapshots?
clusterArn=clusterArn&maxResults=maxResults&nextToken=nextToken&snapshotType=snapshotType
 HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

clusterArn

El identificador ARN del clúster elástico.

maxResults

El número máximo de resultados de instantáneas de clúster elástico que se reciben en la respuesta.

Rango válido: valor mínimo de 20. Valor máximo de 100.

nextToken

Un token de paginación proporcionado por una solicitud anterior. Si se especifica este parámetro, la respuesta solo incluye registros más allá del token, hasta el valor especificado por `max-results`.

Si no hay más datos en la respuesta, no se devolverá el `nextToken`.

snapshotType

El tipo de instantáneas del clúster que se van a devolver. Puede especificar uno de los siguientes valores:

- `automated`: devuelve todas las instantáneas del clúster que Amazon DocumentDB haya creado automáticamente para su cuenta de AWS.
- `manual`: devuelve todas las instantáneas del clúster que haya creado manualmente para su cuenta de AWS.

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
   "nextToken": "string",
   "snapshots": [
      {
         "clusterArn": "string",
         "snapshotArn": "string",
         "snapshotCreationTime": "string",
         "snapshotName": "string",
         "status": "string"
      }
   ]
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

nextToken

Un token de paginación proporcionado por una solicitud anterior. Si se especifica este parámetro, la respuesta solo incluye registros más allá del token, hasta el valor especificado por `max-results`.

Si no hay más datos en la respuesta, no se devolverá el `nextToken`.

Tipo: cadena

snapshots

Una lista de instantáneas de un clúster elástico específico.

Tipo: matriz de objetos ClusterSnapshotInList

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

AccessDeniedException

Una excepción que se produce cuando no hay permisos suficientes para realizar una acción.

message

Un mensaje de error que explica por qué se denegó el acceso.

Código de estado HTTP: 403

InternalServerException

Se ha producido un error en el servidor interno.

Código de estado HTTP: 500

ThrottlingException

Se lanzará ThrottlingException cuando se deniegue la solicitud debido a la limitación de la solicitud.

retryAfterSeconds

La cantidad de segundos que se debe esperar para volver a intentar la operación.

Código de estado HTTP: 429

ValidationException

Estructura que define una excepción de validación.

fieldList

Una lista de los campos en los que se produjo la excepción de validación.

message

Un mensaje de error que describe la excepción de validación.

reason

El motivo por el que se produjo la excepción de validación (uno de los siguientes: `unknownOperation`, `cannotParse`, `fieldValidationFailed` o `other`).

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

ListPendingMaintenanceActions

Servicio: Amazon DocumentDB Elastic Clusters

Recupera una lista de todas las acciones de mantenimiento pendientes.

Sintaxis de la solicitud

```
GET /pending-actions?maxResults=maxResults&nextToken=nextToken HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

maxResults

El número máximo de registros que se debe incluir en la respuesta. Si el número de registros es superior al valor `maxResults` especificado, se incluye en la respuesta un token de paginación (marcador) de modo que se puedan recuperar el resto de los resultados.

Rango válido: valor mínimo de 1. Valor máximo de 100.

nextToken

Un token de paginación opcional proporcionado por una solicitud anterior. Si se especifica este parámetro, la respuesta solo incluye registros más allá del marcador, hasta el valor especificado por `maxResults`.

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
   "nextToken": "string",
   "resourcePendingMaintenanceActions": [
      {
         "pendingMaintenanceActionDetails": [
```

```
            {
               "action": "string",
               "autoAppliedAfterDate": "string",
               "currentApplyDate": "string",
               "description": "string",
               "forcedApplyDate": "string",
               "optInStatus": "string"
            }
         ],
         "resourceArn": "string"
      }
   ]
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

resourcePendingMaintenanceActions

Proporciona información acerca de una acción de mantenimiento pendiente para un recurso.

Tipo: matriz de objetos ResourcePendingMaintenanceAction

nextToken

Un token de paginación opcional proporcionado por una solicitud anterior. Si se muestra este parámetro, las respuestas solo incluyen registros más allá del marcador, hasta el valor especificado por `maxResults`.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

AccessDeniedException

Una excepción que se produce cuando no hay permisos suficientes para realizar una acción.

message

Un mensaje de error que explica por qué se denegó el acceso.

Código de estado HTTP: 403

InternalServerException

Se ha producido un error en el servidor interno.

Código de estado HTTP: 500

ThrottlingException

Se lanzará ThrottlingException cuando se deniegue la solicitud debido a la limitación de la solicitud.

retryAfterSeconds

La cantidad de segundos que se debe esperar para volver a intentar la operación.

Código de estado HTTP: 429

ValidationException

Estructura que define una excepción de validación.

fieldList

Una lista de los campos en los que se produjo la excepción de validación.

message

Un mensaje de error que describe la excepción de validación.

reason

El motivo por el que se produjo la excepción de validación (uno de los siguientes: `unknownOperation`, `cannotParse`, `fieldValidationFailed` o `other`).

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

ListTagsForResource

Servicio: Amazon DocumentDB Elastic Clusters

Enumera todas las etiquetas de un recurso de clúster elástico

Sintaxis de la solicitud

```
GET /tags/resourceArn HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

resourceArn

El identificador de ARN del recurso de clúster elástico.

Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 1011.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
   "tags": {
      "string" : "string"
   }
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

tags

La lista de etiquetas del recurso de clúster elástico especificado.

Tipo: mapa de cadena a cadena

Limitaciones de longitud de la clave: longitud mínima de 1. Longitud máxima de 128.

Patrón de clave: `(?!aws:)[a-zA-Z+-=._:/]+`

Limitaciones de longitud de los valores: longitud mínima de 0. La longitud máxima es de 256 caracteres.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServerException

Se ha producido un error en el servidor interno.

Código de estado HTTP: 500

ResourceNotFoundException

No se pudo encontrar el recurso especificado.

message

Un mensaje de error que describe el error.

resourceId

El identificador del recurso que no se pudo encontrar.

resourceType

El tipo del recurso que no se pudo encontrar.

Código de estado HTTP: 404

ThrottlingException

Se lanzará ThrottlingException cuando se deniegue la solicitud debido a la limitación de la solicitud.

retryAfterSeconds

La cantidad de segundos que se debe esperar para volver a intentar la operación.

Código de estado HTTP: 429

ValidationException

Estructura que define una excepción de validación.

fieldList

Una lista de los campos en los que se produjo la excepción de validación.

message

Un mensaje de error que describe la excepción de validación.

reason

El motivo por el que se produjo la excepción de validación (uno de los siguientes: `unknownOperation`, `cannotParse`, `fieldValidationFailed` o `other`).

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

RestoreClusterFromSnapshot

Servicio: Amazon DocumentDB Elastic Clusters

Restaura un clúster elástico desde una instantánea.

Sintaxis de la solicitud

```
POST /cluster-snapshot/snapshotArn/restore HTTP/1.1
Content-type: application/json

{
   "clusterName": "string",
   "kmsKeyId": "string",
   "shardCapacity": number,
   "shardInstanceCount": number,
   "subnetIds": [ "string" ],
   "tags": {
      "string" : "string"
   },
   "vpcSecurityGroupIds": [ "string" ]
}
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

snapshotArn

El identificador ARN de la instantánea del clúster elástico.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

clusterName

El nombre del clúster elástico.

Tipo: cadena

Obligatorio: sí

kmsKeyId

El identificador de clave de KMS que se debe utilizar para cifrar el nuevo clúster elástico de Amazon DocumentDB.

El identificador de la clave de KMS es el Nombre de recurso de Amazon (ARN) de la clave de cifrado de KMS. Si está creando un clúster con la misma cuenta de Amazon a la que pertenece esta clave de cifrado de KMS, puede utilizar el alias de la clave de KMS en lugar del ARN como clave de cifrado de KMS.

Si no se especifica una clave de cifrado, Amazon DocumentDB utiliza la clave de cifrado predeterminada que KMS crea para la cuenta. Su cuenta dispone de una clave de cifrado predeterminada diferente para cada región de Amazon.

Tipo: cadena

Requerido: no

shardCapacity

La capacidad de cada partición del nuevo clúster elástico restaurado.

Tipo: entero

Obligatorio: no

shardInstanceCount

El número de instancias de réplica que se aplica a todas las particiones del clúster elástico. Un valor de `shardInstanceCount` igual a 1 significa que hay una instancia de escritura y las instancias adicionales son réplicas que se pueden usar para llevar a cabo lecturas y mejorar la disponibilidad.

Tipo: entero

Obligatorio: no

subnetIds

Los ID de subredes de Amazon EC2 para el clúster elástico.

Tipo: matriz de cadenas

Obligatorio: no

tags

Una lista de los nombres de etiquetas que se van a asignar al clúster elástico restaurado, en forma de una matriz de pares clave-valor, en la que la clave es el nombre de la etiqueta y el valor es el valor de la clave.

Tipo: mapa de cadena a cadena

Limitaciones de longitud de la clave: longitud mínima de 1. Longitud máxima de 128.

Patrón de clave: `(?!aws:)[a-zA-Z+-=._:/]+`

Limitaciones de longitud de los valores: longitud mínima de 0. La longitud máxima es de 256 caracteres.

Obligatorio: no

vpcSecurityGroupIds

Una lista de grupos de seguridad de VPC de EC2 para asociar al clúster elástico.

Tipo: matriz de cadenas

Obligatorio: no

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
   "cluster": {
      "adminUserName": "string",
      "authType": "string",
      "backupRetentionPeriod": number,
      "clusterArn": "string",
      "clusterEndpoint": "string",
      "clusterName": "string",
      "createTime": "string",
      "kmsKeyId": "string",
      "preferredBackupWindow": "string",
      "preferredMaintenanceWindow": "string",
      "shardCapacity": number,
      "shardCount": number,
```

```
      "shardInstanceCount": number,
      "shards": [
         {
            "createTime": "string",
            "shardId": "string",
            "status": "string"
         }
      ],
      "status": "string",
      "subnetIds": [ "string" ],
      "vpcSecurityGroupIds": [ "string" ]
   }
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

cluster

Devuelve información sobre el clúster elástico restaurado.

Tipo: objeto Cluster

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

AccessDeniedException

Una excepción que se produce cuando no hay permisos suficientes para realizar una acción.

message

Un mensaje de error que explica por qué se denegó el acceso.

Código de estado HTTP: 403

ConflictException

Se ha producido un conflicto de acceso.

resourceId

El identificador del recurso en el que se produjo un conflicto de acceso.

resourceType

El tipo del recurso en el que se produjo un conflicto de acceso.

Código de estado HTTP: 409

InternalServerException

Se ha producido un error en el servidor interno.

Código de estado HTTP: 500

ResourceNotFoundException

No se pudo encontrar el recurso especificado.

message

Un mensaje de error que describe el error.

resourceId

El identificador del recurso que no se pudo encontrar.

resourceType

El tipo del recurso que no se pudo encontrar.

Código de estado HTTP: 404

ServiceQuotaExceededException

Se ha superado la cuota de servicio para la acción.

Código de estado HTTP: 402

ThrottlingException

Se lanzará ThrottlingException cuando se deniegue la solicitud debido a la limitación de la solicitud.

retryAfterSeconds

La cantidad de segundos que se debe esperar para volver a intentar la operación.

Código de estado HTTP: 429

ValidationException

Estructura que define una excepción de validación.

fieldList

Una lista de los campos en los que se produjo la excepción de validación.

message

Un mensaje de error que describe la excepción de validación.

reason

El motivo por el que se produjo la excepción de validación (uno de los siguientes: `unknownOperation`, `cannotParse`, `fieldValidationFailed` o `other`).

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK de para Ruby V3

StartCluster

Servicio: Amazon DocumentDB Elastic Clusters

Reinicia el clúster elástico detenido que está especificado por `clusterARN`.

Sintaxis de la solicitud

```
POST /cluster/clusterArn/start HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

clusterArn

El identificador ARN del clúster elástico.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
   "cluster": {
      "adminUserName": "string",
      "authType": "string",
      "backupRetentionPeriod": number,
      "clusterArn": "string",
      "clusterEndpoint": "string",
      "clusterName": "string",
      "createTime": "string",
      "kmsKeyId": "string",
      "preferredBackupWindow": "string",
      "preferredMaintenanceWindow": "string",
      "shardCapacity": number,
      "shardCount": number,
```

```
      "shardInstanceCount": number,
      "shards": [
         {
            "createTime": "string",
            "shardId": "string",
            "status": "string"
         }
      ],
      "status": "string",
      "subnetIds": [ "string" ],
      "vpcSecurityGroupIds": [ "string" ]
   }
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

cluster

Devuelve información sobre un clúster elástico específico.

Tipo: objeto Cluster

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

AccessDeniedException

Una excepción que se produce cuando no hay permisos suficientes para realizar una acción.

message

Un mensaje de error que explica por qué se denegó el acceso.

Código de estado HTTP: 403

InternalServerException

Se ha producido un error en el servidor interno.

Código de estado HTTP: 500

ResourceNotFoundException

No se pudo encontrar el recurso especificado.

message

Un mensaje de error que describe el error.

resourceId

El identificador del recurso que no se pudo encontrar.

resourceType

El tipo del recurso que no se pudo encontrar.

Código de estado HTTP: 404

ThrottlingException

Se lanzará ThrottlingException cuando se deniegue la solicitud debido a la limitación de la solicitud.

retryAfterSeconds

La cantidad de segundos que se debe esperar para volver a intentar la operación.

Código de estado HTTP: 429

ValidationException

Estructura que define una excepción de validación.

fieldList

Una lista de los campos en los que se produjo la excepción de validación.

message

Un mensaje de error que describe la excepción de validación.

reason

El motivo por el que se produjo la excepción de validación (uno de los siguientes: `unknownOperation`, `cannotParse`, `fieldValidationFailed` o `other`).

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

StopCluster

Servicio: Amazon DocumentDB Elastic Clusters

Detiene el clúster elástico en ejecución especificado por `clusterArn`. El estado del clúster elástico debe ser disponible.

Sintaxis de la solicitud

```
POST /cluster/clusterArn/stop HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

clusterArn

El identificador ARN del clúster elástico.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
   "cluster": {
      "adminUserName": "string",
      "authType": "string",
      "backupRetentionPeriod": number,
      "clusterArn": "string",
      "clusterEndpoint": "string",
      "clusterName": "string",
      "createTime": "string",
      "kmsKeyId": "string",
      "preferredBackupWindow": "string",
      "preferredMaintenanceWindow": "string",
      "shardCapacity": number,
```

```
      "shardCount": number,
      "shardInstanceCount": number,
      "shards": [
         {
            "createTime": "string",
            "shardId": "string",
            "status": "string"
         }
      ],
      "status": "string",
      "subnetIds": [ "string" ],
      "vpcSecurityGroupIds": [ "string" ]
   }
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

cluster

Devuelve información sobre un clúster elástico específico.

Tipo: objeto Cluster

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

AccessDeniedException

Una excepción que se produce cuando no hay permisos suficientes para realizar una acción.

message

Un mensaje de error que explica por qué se denegó el acceso.

Código de estado HTTP: 403

InternalServerException

Se ha producido un error en el servidor interno.

Código de estado HTTP: 500

ResourceNotFoundException

No se pudo encontrar el recurso especificado.

message

Un mensaje de error que describe el error.

resourceId

El identificador del recurso que no se pudo encontrar.

resourceType

El tipo del recurso que no se pudo encontrar.

Código de estado HTTP: 404

ThrottlingException

Se lanzará ThrottlingException cuando se deniegue la solicitud debido a la limitación de la solicitud.

retryAfterSeconds

La cantidad de segundos que se debe esperar para volver a intentar la operación.

Código de estado HTTP: 429

ValidationException

Estructura que define una excepción de validación.

fieldList

Una lista de los campos en los que se produjo la excepción de validación.

message

Un mensaje de error que describe la excepción de validación.

reason

El motivo por el que se produjo la excepción de validación (uno de los siguientes: `unknownOperation`, `cannotParse`, `fieldValidationFailed` o `other`).

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK para Ruby V3

TagResource

Servicio: Amazon DocumentDB Elastic Clusters

Añade etiquetas de metadatos a un recurso de clúster elástico

Sintaxis de la solicitud

```
POST /tags/resourceArn HTTP/1.1
Content-type: application/json

{
   "tags": {
      "string" : "string"
   }
}
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

resourceArn

El identificador de ARN del recurso de clúster elástico.

Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 1011.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

tags

Las etiquetas asignadas al recurso de clúster elástico.

Tipo: mapa de cadena a cadena

Limitaciones de longitud de la clave: longitud mínima de 1. Longitud máxima de 128.

Patrón de clave: `(?!aws:)[a-zA-Z+-=._:/]+`

Limitaciones de longitud de los valores: longitud mínima de 0. La longitud máxima es de 256 caracteres.

Obligatorio: sí

Sintaxis de la respuesta

```
HTTP/1.1 200
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServerException

Se ha producido un error en el servidor interno.

Código de estado HTTP: 500

ResourceNotFoundException

No se pudo encontrar el recurso especificado.

message

Un mensaje de error que describe el error.

resourceId

El identificador del recurso que no se pudo encontrar.

resourceType

El tipo del recurso que no se pudo encontrar.

Código de estado HTTP: 404

ThrottlingException

Se lanzará ThrottlingException cuando se deniegue la solicitud debido a la limitación de la solicitud.

retryAfterSeconds

La cantidad de segundos que se debe esperar para volver a intentar la operación.

Código de estado HTTP: 429

ValidationException

Estructura que define una excepción de validación.

fieldList

Una lista de los campos en los que se produjo la excepción de validación.

message

Un mensaje de error que describe la excepción de validación.

reason

El motivo por el que se produjo la excepción de validación (uno de los siguientes: `unknownOperation`, `cannotParse`, `fieldValidationFailed` o `other`).

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin

- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK de para Ruby V3

UntagResource

Servicio: Amazon DocumentDB Elastic Clusters

Elimina etiquetas de metadatos de un recurso de clúster elástico

Sintaxis de la solicitud

```
DELETE /tags/resourceArn?tagKeys=tagKeys HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

resourceArn

El identificador de ARN del recurso de clúster elástico.

Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 1011.

Obligatorio: sí

tagKeys

Las claves de etiqueta que se van a eliminar del recurso de clúster elástico.

Miembros de la matriz: número mínimo de 0 artículos. Número máximo de 50 artículos.

Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 128.

Patrón: `(?!aws:)[a-zA-Z+-=._:/]+`

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServerException

Se ha producido un error en el servidor interno.

Código de estado HTTP: 500

ResourceNotFoundException

No se pudo encontrar el recurso especificado.

message

Un mensaje de error que describe el error.

resourceId

El identificador del recurso que no se pudo encontrar.

resourceType

El tipo del recurso que no se pudo encontrar.

Código de estado HTTP: 404

ThrottlingException

Se lanzará ThrottlingException cuando se deniegue la solicitud debido a la limitación de la solicitud.

retryAfterSeconds

La cantidad de segundos que se debe esperar para volver a intentar la operación.

Código de estado HTTP: 429

ValidationException

Estructura que define una excepción de validación.

fieldList

Una lista de los campos en los que se produjo la excepción de validación.

message

Un mensaje de error que describe la excepción de validación.

reason

El motivo por el que se produjo la excepción de validación (uno de los siguientes: `unknownOperation`, `cannotParse`, `fieldValidationFailed` o `other`).

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK de para Ruby V3

UpdateCluster

Servicio: Amazon DocumentDB Elastic Clusters

Modifica un clúster elástico. Esto incluye actualizar el nombre de usuario y la contraseña del administrador, actualizar la versión de la API y configurar una ventana de copia de seguridad y una ventana de mantenimiento

Sintaxis de la solicitud

```
PUT /cluster/clusterArn HTTP/1.1
Content-type: application/json

{
   "adminUserPassword": "string",
   "authType": "string",
   "backupRetentionPeriod": number,
   "clientToken": "string",
   "preferredBackupWindow": "string",
   "preferredMaintenanceWindow": "string",
   "shardCapacity": number,
   "shardCount": number,
   "shardInstanceCount": number,
   "subnetIds": [ "string" ],
   "vpcSecurityGroupIds": [ "string" ]
}
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

clusterArn

El identificador ARN del clúster elástico.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

adminUserPassword

La contraseña asociada al administrador del clúster elástico. Esta contraseña puede contener cualquier carácter ASCII imprimible, excepto barra inclinada (/), comillas dobles (") o el símbolo de “arroba” (@).

Limitaciones: debe contener de 8 a 100 caracteres.

Tipo: cadena

Requerido: no

authType

El tipo de autenticación utilizado para determinar dónde buscar la contraseña que se usa para acceder al clúster elástico. Los tipos válidos son `PLAIN_TEXT` o `SECRET_ARN`.

Tipo: cadena

Valores válidos: `PLAIN_TEXT | SECRET_ARN`

Obligatorio: no

backupRetentionPeriod

El número de días durante los que se conservan las instantáneas de base de datos automáticas.

Tipo: entero

Obligatorio: no

clientToken

El token de cliente del clúster elástico.

Tipo: cadena

Requerido: no

preferredBackupWindow

El intervalo de tiempo diario durante el que se crean las copias de seguridad automatizadas si las copias de seguridad automatizadas están habilitadas según lo determina `backupRetentionPeriod`.

Tipo: cadena

Requerido: no

preferredMaintenanceWindow

El intervalo de tiempo semanal durante el cual puede llevarse a cabo el mantenimiento del sistema, en tiempo universal coordinado (UTC).

Formato: `ddd:hh24:mi-ddd:hh24:mi`

El valor predeterminado es un periodo de 30 minutos seleccionado al azar de un bloque de 8 horas de tiempo para cada Región de AWS, que tiene lugar un día de la semana al azar.

Días válidos: lunes, martes, miércoles, jueves, viernes, sábado, domingo

Restricciones: plazo mínimo de 30 minutos.

Tipo: cadena

Requerido: no

shardCapacity

La cantidad de vCPU asignadas a cada partición de clúster elástico. El máximo es 64. Los valores permitidos son 2, 4, 8, 16, 32, 64.

Tipo: entero

Obligatorio: no

shardCount

El número de particiones asignadas al clúster elástico. El máximo es 32.

Tipo: entero

Obligatorio: no

shardInstanceCount

El número de instancias de réplica que se aplica a todas las particiones del clúster elástico. Un valor de `shardInstanceCount` igual a 1 significa que hay una instancia de escritura y las instancias adicionales son réplicas que se pueden usar para llevar a cabo lecturas y mejorar la disponibilidad.

Tipo: entero

Obligatorio: no

subnetIds

Los ID de subredes de Amazon EC2 para el clúster elástico.

Tipo: matriz de cadenas

Obligatorio: no

vpcSecurityGroupIds

Una lista de grupos de seguridad de VPC de EC2 para asociar al clúster elástico.

Tipo: matriz de cadenas

Obligatorio: no

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
   "cluster": {
      "adminUserName": "string",
      "authType": "string",
      "backupRetentionPeriod": number,
      "clusterArn": "string",
      "clusterEndpoint": "string",
      "clusterName": "string",
      "createTime": "string",
      "kmsKeyId": "string",
      "preferredBackupWindow": "string",
      "preferredMaintenanceWindow": "string",
      "shardCapacity": number,
      "shardCount": number,
      "shardInstanceCount": number,
      "shards": [
         {
            "createTime": "string",
            "shardId": "string",
            "status": "string"
         }
```

```
      ],
      "status": "string",
      "subnetIds": [ "string" ],
      "vpcSecurityGroupIds": [ "string" ]
   }
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

cluster

Devuelve información sobre el clúster elástico actualizado.

Tipo: objeto Cluster

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

AccessDeniedException

Una excepción que se produce cuando no hay permisos suficientes para realizar una acción.

message

Un mensaje de error que explica por qué se denegó el acceso.

Código de estado HTTP: 403

ConflictException

Se ha producido un conflicto de acceso.

resourceId

El identificador del recurso en el que se produjo un conflicto de acceso.

resourceType

El tipo del recurso en el que se produjo un conflicto de acceso.

Código de estado HTTP: 409

InternalServerException

Se ha producido un error en el servidor interno.

Código de estado HTTP: 500

ResourceNotFoundException

No se pudo encontrar el recurso especificado.

message

Un mensaje de error que describe el error.

resourceId

El identificador del recurso que no se pudo encontrar.

resourceType

El tipo del recurso que no se pudo encontrar.

Código de estado HTTP: 404

ThrottlingException

Se lanzará ThrottlingException cuando se deniegue la solicitud debido a la limitación de la solicitud.

retryAfterSeconds

La cantidad de segundos que se debe esperar para volver a intentar la operación.

Código de estado HTTP: 429

ValidationException

Estructura que define una excepción de validación.

fieldList

Una lista de los campos en los que se produjo la excepción de validación.

message

Un mensaje de error que describe la excepción de validación.

reason

El motivo por el que se produjo la excepción de validación (uno de los siguientes: `unknownOperation`, `cannotParse`, `fieldValidationFailed` o `other`).

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- Interfaz de la línea de comandos de AWS, versión 2
- AWS SDK de para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK de para Kotlin
- AWS SDK de para PHP V3
- AWS SDK de para Python
- AWS SDK de para Ruby V3

Data Types

admite los siguientes tipos de datos Amazon DocumentDB (with MongoDB compatibility):

- AvailabilityZone
- Certificate
- CertificateDetails
- CloudwatchLogsExportConfiguration
- ClusterMasterUserSecret
- DBCluster
- DBClusterMember

- DBClusterParameterGroup
- DBClusterRole
- DBClusterSnapshot
- DBClusterSnapshotAttribute
- DBClusterSnapshotAttributesResult
- DBEngineVersion
- DBInstance
- DBInstanceStatusInfo
- DBSubnetGroup
- Endpoint
- EngineDefaults
- Event
- EventCategoriesMap
- EventSubscription
- Filter
- GlobalCluster
- GlobalClusterMember
- OrderableDBInstanceOption
- Parameter
- PendingCloudwatchLogsExports
- PendingMaintenanceAction
- PendingModifiedValues
- ResourcePendingMaintenanceActions
- ServerlessV2FeaturesSupport
- ServerlessV2ScalingConfiguration
- ServerlessV2ScalingConfigurationInfo
- Subnet
- Tag
- UpgradeTarget
- VpcSecurityGroupMembership

Los siguientes tipos de datos son compatibles con los clústeres elásticos de Amazon DocumentDB:

- Cluster
- ClusterInList
- ClusterSnapshot
- ClusterSnapshotInList
- PendingMaintenanceActionDetails
- ResourcePendingMaintenanceAction
- Shard
- ValidationExceptionField

Amazon DocumentDB (with MongoDB compatibility)

admite los siguientes tipos de datos Amazon DocumentDB (with MongoDB compatibility):

- AvailabilityZone
- Certificate
- CertificateDetails
- CloudwatchLogsExportConfiguration
- ClusterMasterUserSecret
- DBCluster
- DBClusterMember
- DBClusterParameterGroup
- DBClusterRole
- DBClusterSnapshot
- DBClusterSnapshotAttribute
- DBClusterSnapshotAttributesResult
- DBEngineVersion
- DBInstance
- DBInstanceStatusInfo
- DBSubnetGroup
- Endpoint

- EngineDefaults
- Event
- EventCategoriesMap
- EventSubscription
- Filter
- GlobalCluster
- GlobalClusterMember
- OrderableDBInstanceOption
- Parameter
- PendingCloudwatchLogsExports
- PendingMaintenanceAction
- PendingModifiedValues
- ResourcePendingMaintenanceActions
- ServerlessV2FeaturesSupport
- ServerlessV2ScalingConfiguration
- ServerlessV2ScalingConfigurationInfo
- Subnet
- Tag
- UpgradeTarget
- VpcSecurityGroupMembership

AvailabilityZone

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Información sobre una zona de disponibilidad.

Contenido

> **Note**
>
> Los parámetros obligatorios se describen primero en la siguiente tabla.

Name

El nombre de la zona de disponibilidad.

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

Certificate

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Certificado de una entidad de certificación (CA) para una Cuenta de AWS.

Contenido

> **Note**
>
> Los parámetros obligatorios se describen primero en la siguiente tabla.

CertificateArn

El nombre de recurso de Amazon (ARN) para el certificado.

Ejemplo:: `arn:aws:rds:us-east-1::cert:rds-ca-2019`

Tipo: cadena

Requerido: no

CertificateIdentifier

La clave única que identifica un certificado.

Ejemplo:: `rds-ca-2019`

Tipo: cadena

Requerido: no

CertificateType

Escriba el nombre del certificado.

Ejemplo:: `CA`

Tipo: cadena

Requerido: no

Thumbprint

La huella digital del certificado.

Tipo: cadena

Requerido: no

ValidFrom

La fecha y hora de inicio a partir de la cual el certificado es válido.

Ejemplo:: `2019-07-31T17:57:09Z`

Tipo: marca temporal

Obligatorio: no

ValidTill

La fecha y hora después de la cual el certificado no es válido.

Ejemplo:: `2024-07-31T17:57:09Z`

Tipo: marca temporal

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

CertificateDetails

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Devuelve los detalles del certificado de servidor de la instancia de base de datos.

Para obtener más información, consulte Cómo actualizar los certificados TLS de Amazon DocumentDB y Cómo cifrar datos en tránsito en la Guía para desarrolladores de Amazon DocumentDB.

Contenido

> **Note**
>
> Los parámetros obligatorios se describen primero en la siguiente tabla.

CAIdentifier

El identificador CA del certificado de CA que usado para el certificado de servidor de la instancia de base de datos.

Tipo: cadena

Requerido: no

ValidTill

La fecha de vencimiento del certificado de servidor de la instancia de base de datos.

Tipo: marca temporal

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

CloudwatchLogsExportConfiguration

Servicio: Amazon DocumentDB (with MongoDB compatibility)

La opción de configuración para los tipos de registro que se debe habilitar para la exportación a Registros de Amazon CloudWatch para una instancia o un clúster específico.

Las matrices `EnableLogTypes` y `DisableLogTypes` determinan qué registros se exportarán (o no) a CloudWatch Logs. Los valores de estas matrices dependen del motor que se utilice.

Contenido

> **Note**
>
> Los parámetros obligatorios se describen primero en la siguiente tabla.

DisableLogTypes.member.N

La lista de tipos de registros que desea deshabilitar.

Tipo: matriz de cadenas

Obligatorio: no

EnableLogTypes.member.N

La lista de tipos de registros que desea habilitar.

Tipo: matriz de cadenas

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

ClusterMasterUserSecret

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Contiene el secreto administrado por Amazon DocumentDB en Secrets Manager de AWS para la contraseña del usuario maestro.

Contenido

> **Note**
>
> Los parámetros obligatorios se describen primero en la siguiente tabla.

KmsKeyId

El identificador de la clave de AWS KMS que se utiliza para cifrar el secreto.

Tipo: cadena

Requerido: no

SecretArn

El nombre de recurso de Amazon (ARN) del secreto.

Tipo: cadena

Requerido: no

SecretStatus

El estado del secreto.

Otros valores de estado posibles son:

- en creación: se está creando el secreto.
- activo: el secreto está disponible para su uso y rotación normales.
- en rotación: se está rotando el secreto.
- dañado: el secreto se puede usar para acceder a las credenciales de la base de datos, pero no se puede rotar. Un secreto puede tener este estado si, por ejemplo, se cambian los permisos para que Amazon DocumentDB ya no pueda acceder al secreto ni a la clave de KMS del secreto.

Cuando un secreto tiene este estado, puede corregir la condición que provocó el estado. De forma alternativa, modifique la instancia para desactivar la administración automática de las credenciales de la base de datos y, a continuación, modifique la instancia para activar la administración automática de las credenciales de la base de datos.

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

DBCluster

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Información detallada sobre un clúster.

Contenido

> **Note**
>
> Los parámetros obligatorios se describen primero en la siguiente tabla.

AssociatedRoles.DBClusterRole.N

Proporciona una lista de los roles AWS Identity and Access Management (IAM) que están asociados con un clúster de base de datos. Los roles de IAM asociados a un clúster conceden permisos para que dicho clúster acceda a otros servicios de AWS en su nombre.

Tipo: matriz de objetos DBClusterRole

Obligatorio: no

AvailabilityZones.AvailabilityZone.N

Proporciona la lista de zonas de disponibilidad de Amazon EC2 en las que se pueden crear instancias en el clúster.

Tipo: matriz de cadenas

Obligatorio: no

BackupRetentionPeriod

Especifica el número de días durante los que se retienen las instantáneas automáticas.

Tipo: entero

Obligatorio: no

CloneGroupId

Identifica el grupo de clones al que está asociado el clúster de base de datos.

Tipo: cadena

Requerido: no

ClusterCreateTime

Especifica la hora a la que se creó el clúster, en tiempo universal coordinado (UTC).

Tipo: marca temporal

Obligatorio: no

DBClusterArn

El Nombre de recurso de Amazon (ARN) para el clúster.

Tipo: cadena

Requerido: no

DBClusterIdentifier

Contiene un identificador de clúster suministrado por el usuario. Este identificador es la clave única que identifica un clúster.

Tipo: cadena

Requerido: no

DBClusterMembers.DBClusterMember.N

Proporciona la lista de instancias que componen el clúster.

Tipo: matriz de objetos DBClusterMember

Obligatorio: no

DBClusterParameterGroup

Especifica el nombre del grupo de parámetros de clúster para el clúster.

Tipo: cadena

Requerido: no

DbClusterResourceId

El identificador inmutable único de Región de AWS para el clúster. Este identificador se encuentra en las entradas de registro de AWS CloudTrail cada vez que se accede a la clave de AWS KMS del clúster.

Tipo: cadena

Requerido: no

DBSubnetGroup

Especifica información sobre el grupo de subred asociado con el clúster, incluido el nombre, la descripción y subredes en el grupo de subred.

Tipo: cadena

Requerido: no

DeletionProtection

Especifica si se puede eliminar este clúster. Si `DeletionProtection` está habilitado, no se puede eliminar el clúster a menos que se modifique y `DeletionProtection` esté deshabilitado. `DeletionProtection` protege los clústeres de una eliminación accidental.

Tipo: Booleano

Obligatorio: no

EarliestRestorableTime

Especifica la última hora a la que se puede restaurar una base de datos con la restauración de un punto en el tiempo.

Tipo: marca temporal

Obligatorio: no

EnabledCloudwatchLogsExports.member.N

Una lista de tipos de registro para los que este clúster está configurado para exportar a los Registros de Amazon CloudWatch.

Tipo: matriz de cadenas

Obligatorio: no

Endpoint

Especifica el punto de conexión para la instancia principal del clúster.

Tipo: cadena

Requerido: no

Engine

Proporciona el nombre del motor de base de datos que se debe utilizar para este clúster.

Tipo: cadena

Requerido: no

EngineVersion

Indica la versión del motor de base de datos.

Tipo: cadena

Requerido: no

HostedZoneId

Especifica el ID que Amazon Route 53 asigna al crear una zona alojada.

Tipo: cadena

Requerido: no

IOOptimizedNextAllowedModificationTime

La próxima vez, podrá modificar el clúster de Amazon DocumentDB para utilizar el tipo de almacenamiento iopt1.

Tipo: marca temporal

Obligatorio: no

KmsKeyId

Si `StorageEncrypted` es `true`, el identificador de la clave de AWS KMS para el clúster cifrado.

Tipo: cadena

Requerido: no

LatestRestorableTime

Especifica la última hora a la que se puede restaurar una base de datos con la restauración de un punto en el tiempo.

Tipo: marca temporal

Obligatorio: no

MasterUsername

Contiene el nombre de usuario maestro para el clúster.

Tipo: cadena

Requerido: no

MasterUserSecret

El secreto administrado por Amazon DocumentDB en Secrets Manager de AWS para la contraseña del usuario maestro.

Tipo: objeto ClusterMasterUserSecret

Obligatorio: no

MultiAZ

Especifica si el clúster tiene instancias en varias zonas de disponibilidad.

Tipo: Booleano

Obligatorio: no

NetworkType

El tipo de red del clúster.

El tipo de red viene determinado por el `DBSubnetGroup` especificado para el clúster. Un `DBSubnetGroup` admite solamente el protocolo IPv4 o los protocolos IPv4 e IPv6 (`DUAL`).

Para obtener más información, consulte Clústeres de DocumentDB en una VPC en la Guía para desarrolladores de Amazon DocumentDB.

Valores válidos: `IPV4` | `DUAL`

Tipo: cadena

Requerido: no

PercentProgress

Especifica el progreso de la operación como porcentaje.

Tipo: cadena

Requerido: no

Port

Especifica el puerto en el que escucha el motor de la base de datos.

Tipo: entero

Obligatorio: no

PreferredBackupWindow

Especifica el intervalo de tiempo diario durante el cual se crean copias de seguridad automatizadas si las copias de seguridad automatizadas están habilitadas, de acuerdo con la propiedad `BackupRetentionPeriod`.

Tipo: cadena

Requerido: no

PreferredMaintenanceWindow

Especifica el intervalo de tiempo semanal durante el cual puede llevarse a cabo el mantenimiento del sistema, en el horario universal coordinado (UTC).

Tipo: cadena

Requerido: no

ReaderEndpoint

El punto de conexión del lector para el clúster. El punto de conexión del lector de un clúster equilibra la carga de las conexiones entre las réplicas de Amazon DocumentDB que están disponibles en un clúster. A medida que los clientes solicitan nuevas conexiones al punto de conexión del lector, Amazon DocumentDB distribuye las solicitudes de conexión entre las réplicas de Amazon DocumentDB del clúster. Esta funcionalidad puede ayudar a equilibrar la carga de trabajo de lectura entre las distintas réplicas de Amazon DocumentDB del clúster.

Si se produce una conmutación por error y la réplica de Amazon DocumentDB a la que está conectado se convierte en la nueva instancia principal, la conexión se interrumpe. Para seguir enviando la carga de trabajo de lectura a otras réplicas de Amazon DocumentDB del clúster, puede volver a conectarse al punto de conexión del lector.

Tipo: cadena

Requerido: no

ReadReplicaIdentifiers.ReadReplicaIdentifier.N

Contiene uno o más identificadores de los clústeres secundarios asociados a este clúster.

Tipo: matriz de cadenas

Obligatorio: no

ReplicationSourceIdentifier

Contiene el identificador del clúster de origen si este clúster es secundario.

Tipo: cadena

Requerido: no

ServerlessV2ScalingConfiguration

La configuración de escalado de un clúster de Amazon DocumentDB sin servidor.

Tipo: objeto ServerlessV2ScalingConfigurationInfo

Obligatorio: no

Status

Especifica el estado actual de este clúster de base de datos.

Tipo: cadena

Requerido: no

StorageEncrypted

Especifica si el clúster está cifrado.

Tipo: Booleano

Obligatorio: no

StorageType

Tipo de almacenamiento asociado al clúster

Para obtener información sobre los tipos de almacenamiento de los clústeres de Amazon DocumentDB, consulte Cluster storage configurations en la Guía para desarrolladores de Amazon DocumentDB.

Valores válidos para el tipo de almacenamiento: `standard | iopt1`

El valor predeterminado es `standard`

Tipo: cadena

Requerido: no

VpcSecurityGroups.VpcSecurityGroupMembership.N

Una lista de grupos de seguridad de la nube privada virtual (VPC) a las que pertenece el clúster.

Tipo: matriz de objetos VpcSecurityGroupMembership

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

DBClusterMember

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Contiene información sobre una instancia que forma parte de un clúster de base de datos.

Contenido

> **Note**
>
> Los parámetros obligatorios se describen primero en la siguiente tabla.

DBClusterParameterGroupStatus

Especifica el estado del grupo de parámetros de clúster de base de datos para este miembro del clúster de base de datos.

Tipo: cadena

Requerido: no

DBInstanceIdentifier

Especifica el identificador de la instancia de este miembro del clúster.

Tipo: cadena

Requerido: no

IsClusterWriter

El valor que es `true` si el miembro del clúster es la instancia principal del clúster de base de datos y `false` en caso contrario.

Tipo: Booleano

Obligatorio: no

PromotionTier

Valor que especifica el orden en el que se promueve una réplica de Amazon DocumentDB a la instancia primaria tras un fallo de la instancia primaria existente.

Tipo: entero

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

DBClusterParameterGroup

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Información detallada sobre un grupo de parámetros de clúster.

Contenido

> **Note**
>
> Los parámetros obligatorios se describen primero en la siguiente tabla.

DBClusterParameterGroupArn

El Nombre de recurso de Amazon (ARN) para el grupo de parámetros de clúster.

Tipo: cadena

Requerido: no

DBClusterParameterGroupName

Proporciona el nombre del grupo de parámetros de clúster.

Tipo: cadena

Requerido: no

DBParameterGroupFamily

Proporciona el nombre de la familia del grupo de parámetros con el que este grupo de parámetros de clúster es compatible.

Tipo: cadena

Requerido: no

Description

Proporciona la descripción especificada por el usuario para este grupo de parámetros de clúster.

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

DBClusterRole

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Describe un rol de AWS Identity and Access Management (IAM)que está asociado con un clúster de base de datos.

Contenido

> **Note**
>
> Los parámetros obligatorios se describen primero en la siguiente tabla.

RoleArn

El Nombre de recurso de Amazon (ARN) del rol de IAM asociado al clúster de base de datos.

Tipo: cadena

Requerido: no

Status

Describe el estado de asociación entre el rol de IAM y el clúster. La propiedad del `Status` devuelve uno de los siguientes valores:

- `ACTIVE`: el ARN del rol de IAM se asocia con el clúster de base de datos y se puede utilizar para obtener acceso a otros servicios de AWS en su nombre.
- `PENDING`: el ARN del rol de IAM se está asociando al clúster.
- `INVALID`: el ARN del rol de IAM se asocia con el clúster, pero el clúster no puede asumir el rol de IAM para acceder a otros servicios de AWS en su nombre.

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- AWS SDK para C++

- AWS SDK para Java V2
- AWS SDK para Ruby V3

DBClusterSnapshot

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Información detallada sobre una instantánea de un clúster.

Contenido

> **Note**
>
> Los parámetros obligatorios se describen primero en la siguiente tabla.

AvailabilityZones.AvailabilityZone.N

Proporciona la lista de zonas de disponibilidad del EC2 de Amazon donde se pueden restaurar las instancias de la instantánea del clúster.

Tipo: matriz de cadenas

Obligatorio: no

ClusterCreateTime

Especifica la hora a la que se creó el clúster, en tiempo universal coordinado (UTC).

Tipo: marca temporal

Obligatorio: no

DBClusterIdentifier

Especifica el identificador del clúster, del clúster a partir del cual se creó esta instantánea del clúster.

Tipo: cadena

Requerido: no

DBClusterSnapshotArn

El Nombre de recurso de Amazon (ARN) de la instantánea del clúster.

Tipo: cadena

Requerido: no

DBClusterSnapshotIdentifier

Especifica el identificador de la instantánea del clúster.

Tipo: cadena

Requerido: no

Engine

Especifica el nombre del motor de base de datos.

Tipo: cadena

Requerido: no

EngineVersion

Proporciona la versión del motor de base de datos para esta instantánea del clúster.

Tipo: cadena

Requerido: no

KmsKeyId

Si `StorageEncrypted` es `true`, el identificador de la clave de AWS KMS para la instantánea del clúster de base de datos cifrada.

Tipo: cadena

Requerido: no

MasterUsername

Proporciona el nombre de usuario maestro para la instantánea del clúster.

Tipo: cadena

Requerido: no

PercentProgress

Especifica el porcentaje de la estimación de los datos que se han transferido.

Tipo: entero

Obligatorio: no

Port

Especifica el puerto que el clúster estaba escuchando en el momento de la instantánea.

Tipo: entero

Obligatorio: no

SnapshotCreateTime

Proporciona la hora a la que se tomó la instantánea, en UTC.

Tipo: marca temporal

Obligatorio: no

SnapshotType

Proporciona el tipo de instantánea del clúster.

Tipo: cadena

Requerido: no

SourceDBClusterSnapshotArn

Si la instantánea del clúster se ha copiado de una instantánea de clúster de origen, el ARN para la instantánea del clúster de origen; de lo contrario, es un valor nulo.

Tipo: cadena

Requerido: no

Status

Especifica el estado de esta instantánea del clúster.

Tipo: cadena

Requerido: no

StorageEncrypted

Especifica si la instantánea del clúster está cifrada.

Tipo: Booleano

Obligatorio: no

StorageType

Tipo de almacenamiento asociado a la instantánea del clúster

Para obtener información sobre los tipos de almacenamiento de los clústeres de Amazon DocumentDB, consulte Cluster storage configurations en la Guía para desarrolladores de Amazon DocumentDB.

Valores válidos para el tipo de almacenamiento: `standard | iopt1`

El valor predeterminado es `standard`

Tipo: cadena

Requerido: no

VpcId

Otorga el ID de la nube privada virtual (VPC) asociado a la instantánea del clúster.

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

DBClusterSnapshotAttribute

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Contiene el nombre y los valores de un atributo de instantánea del clúster manual.

Los atributos de la instantánea del clúster manual se utilizan para autorizar a otras Cuentas de AWS la restauración de una instantánea de clúster manual.

Contenido

> **Note**
>
> Los parámetros obligatorios se describen primero en la siguiente tabla.

AttributeName

El nombre del atributo de la instantánea del clúster manual.

El atributo llamado `restore` se refiere a la lista de Cuentas de AWS que tienen permiso para copiar o restaurar la instantánea del clúster manual.

Tipo: cadena

Requerido: no

AttributeValues.AttributeValue.N

Los valores del atributo de la instantánea del clúster manual.

Si el campo `AttributeName` se establece en `restore`, este elemento devuelve una lista de ID de Cuentas de AWS con autorización para copiar o restaurar la instantánea del clúster manual. Si el valor de `all` está en la lista, la instantánea del clúster manual es pública y está disponible para cualquier Cuenta de AWS para su copia o restauración.

Tipo: matriz de cadenas

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

DBClusterSnapshotAttributesResult

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Información detallada sobre los atributos asociados a una instantánea de clúster.

Contenido

> **Note**
>
> Los parámetros obligatorios se describen primero en la siguiente tabla.

DBClusterSnapshotAttributes.DBClusterSnapshotAttribute.N

La lista de atributos y valores para la instantánea del clúster.

Tipo: matriz de objetos DBClusterSnapshotAttribute

Obligatorio: no

DBClusterSnapshotIdentifier

El identificador de la instantánea del clúster al que se aplican los atributos.

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

DBEngineVersion

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Información detallada sobre la versión de un motor.

Contenido

> **Note**
>
> Los parámetros obligatorios se describen primero en la siguiente tabla.

DBEngineDescription

La descripción del motor de base de datos.

Tipo: cadena

Requerido: no

DBEngineVersionDescription

La descripción de la versión del motor de base de datos.

Tipo: cadena

Requerido: no

DBParameterGroupFamily

El nombre de la familia de grupos de parámetros para el motor de base de datos.

Tipo: cadena

Requerido: no

Engine

El nombre del motor de base de datos.

Tipo: cadena

Requerido: no

EngineVersion

Número de versión del motor de base de datos.

Tipo: cadena

Requerido: no

ExportableLogTypes.member.N

Los tipos de registros que el motor de base de datos tiene disponibles para la exportación a Registros de Amazon CloudWatch.

Tipo: matriz de cadenas

Obligatorio: no

ServerlessV2FeaturesSupport

Especifica cualquier propiedad o límite de Amazon DocumentDB sin servidor que difiera entre las versiones del motor de Amazon DocumentDB. Puede probar los valores de este atributo cuando decide qué versión de Amazon DocumentDB va a utilizar en un clúster nuevo o actualizado. También puede recuperar la versión de un clúster existente y comprobar si esa versión admite determinadas características de Amazon DocumentDB sin servidor antes de intentar utilizarlas.

Tipo: objeto ServerlessV2FeaturesSupport

Obligatorio: no

SupportedCACertificateIdentifiers.member.N

Una lista de los identificadores de certificados de CA compatibles.

Para obtener más información, consulte Cómo actualizar los certificados TLS de Amazon DocumentDB y Cómo cifrar datos en tránsito en la Guía para desarrolladores de Amazon DocumentDB.

Tipo: matriz de cadenas

Obligatorio: no

SupportsCertificateRotationWithoutRestart

Indica si la versión del motor admite la rotación del certificado del servidor sin reiniciar la instancia de la base de datos.

Tipo: Booleano

Obligatorio: no

SupportsLogExportsToCloudwatchLogs

Un valor que indica si la versión del motor admite la exportación de los tipos de registro especificados por `ExportableLogTypes` a CloudWatch Logs.

Tipo: Booleano

Obligatorio: no

ValidUpgradeTarget.UpgradeTarget.N

Una lista de versiones de motor a la que esta versión del motor de base de datos se puede actualizar.

Tipo: matriz de objetos UpgradeTarget

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

DBInstance

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Información detallada sobre una instancia.

Contenido

> **Note**
>
> Los parámetros obligatorios se describen primero en la siguiente tabla.

AutoMinorVersionUpgrade

No se aplica. Este parámetro no se aplica a Amazon DocumentDB. Amazon DocumentDB no actualiza versiones secundarias, independientemente del valor establecido.

Tipo: Booleano

Obligatorio: no

AvailabilityZone

Especifica el nombre de la Zona de Disponibilidad en la que se encuentra la instancia.

Tipo: cadena

Requerido: no

BackupRetentionPeriod

Especifica el número de días durante los que se retienen las instantáneas automáticas.

Tipo: entero

Obligatorio: no

CACertificateIdentifier

El identificador del certificado de CA para esta instancia de base de datos.

Tipo: cadena

Requerido: no

CertificateDetails

Los detalles del certificado de servidor de la instancia de base de datos.

Tipo: objeto CertificateDetails

Obligatorio: no

CopyTagsToSnapshot

Es un valor que indica si se deben copiar las etiquetas de la instancia de base de datos en instantáneas de la instancia de base de datos. Las etiquetas no se copian de forma predeterminada.

Tipo: Booleano

Obligatorio: no

DBClusterIdentifier

Contiene el nombre del clúster al que pertenece la instancia si ésta es miembro de un clúster.

Tipo: cadena

Requerido: no

DBInstanceArn

El nombre de recurso de Amazon (ARN) de la instancia.

Tipo: cadena

Requerido: no

DBInstanceClass

Contiene el nombre de la clase de capacidad de cómputo y memoria de la instancia.

Tipo: cadena

Requerido: no

DBInstanceIdentifier

Contiene un identificador de base de datos proporcionado por el usuario. Este identificador es la clave única que identifica una instancia.

Tipo: cadena

Requerido: no

DBInstanceStatus

Especifica el estado actual de esta base de datos.

Tipo: cadena

Requerido: no

DbiResourceId

El identificador inmutable único de la Región de AWS para la instancia. Este identificador se encuentra en las entradas de registro de AWS CloudTrail cada vez que se accede a la clave de AWS KMS para la instancia.

Tipo: cadena

Requerido: no

DBSubnetGroup

Especifica información sobre el grupo de subred asociado a la instancia, incluido el nombre, la descripción y subredes en el grupo de subred.

Tipo: objeto DBSubnetGroup

Obligatorio: no

EnabledCloudwatchLogsExports.member.N

Una lista de tipos de registro para los que esta instancia está configurada para exportar a CloudWatch Logs.

Tipo: matriz de cadenas

Obligatorio: no

Endpoint

Especifica el punto de conexión.

Tipo: objeto Endpoint

Obligatorio: no

Engine

Proporciona el nombre del motor de base de datos que se va a usar para esta instancia.

Tipo: cadena

Requerido: no

EngineVersion

Indica la versión del motor de base de datos.

Tipo: cadena

Requerido: no

InstanceCreateTime

Proporciona la fecha y hora en que se creó la instancia.

Tipo: marca temporal

Obligatorio: no

KmsKeyId

Si `StorageEncrypted` es `true`, el identificador de clave AWS KMS para la instancia encriptada.

Tipo: cadena

Requerido: no

LatestRestorableTime

Especifica la última hora a la que se puede restaurar una base de datos con la restauración de un punto en el tiempo.

Tipo: marca temporal

Obligatorio: no

PendingModifiedValues

Especifica que los cambios a la instancia están pendientes. Este elemento solo se incluye cuando los cambios están pendientes. Los cambios específicos se identifican por subelementos.

Tipo: objeto PendingModifiedValues

Obligatorio: no

PerformanceInsightsEnabled

Establézcalo en `true` si la Información de rendimiento de Amazon RDS está habilitada para la instancia de base de datos; de lo contrario, el valor es `false`.

Tipo: Booleano

Obligatorio: no

PerformanceInsightsKMSKeyId

El identificador de la clave de AWS KMS para el cifrado de datos de Performance Insights. El ID de clave de AWS KMS es el nombre de recurso de Amazon (ARN), el identificador de clave de AWS KMS o el alias de clave de AWS KMS de la clave de cifrado de AWS KMS.

Tipo: cadena

Requerido: no

PreferredBackupWindow

Especifica el intervalo de tiempo diario durante el cual se crean copias de seguridad automatizadas si las copias de seguridad automatizadas están habilitadas, de acuerdo con la propiedad `BackupRetentionPeriod`.

Tipo: cadena

Requerido: no

PreferredMaintenanceWindow

Especifica el intervalo de tiempo semanal durante el cual puede llevarse a cabo el mantenimiento del sistema, en el horario universal coordinado (UTC).

Tipo: cadena

Requerido: no

PromotionTier

Valor que especifica el orden en el que se promueve una réplica de Amazon DocumentDB a la instancia primaria tras un fallo de la instancia primaria existente.

Tipo: entero

Obligatorio: no

PubliclyAccessible

No admitido. Actualmente, Amazon DocumentDB no admite puntos de conexión públicos. El valor de `PubliclyAccessible` es siempre `false`.

Tipo: Booleano

Obligatorio: no

StatusInfos.DBInstanceStatusInfo.N

El estado de una réplica de lectura. Si la instancia no es una réplica de lectura, está en blanco.

Tipo: matriz de objetos DBInstanceStatusInfo

Obligatorio: no

StorageEncrypted

Especifica si la instancia está encriptada o no.

Tipo: Booleano

Obligatorio: no

VpcSecurityGroups.VpcSecurityGroupMembership.N

Proporciona una lista de elementos de grupos de seguridad de VPC a la que pertenece la instancia.

Tipo: matriz de objetos VpcSecurityGroupMembership

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- AWS SDK para C++
- AWS SDK para Java V2

- AWS SDK para Ruby V3

DBInstanceStatusInfo

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Proporciona una lista de información de estado para una instancia.

Contenido

> **Note**
>
> Los parámetros obligatorios se describen primero en la siguiente tabla.

Message

Detalles del error si hay un error para la instancia. Si la instancia no se encuentra en un estado de error, este valor aparece en blanco.

Tipo: cadena

Requerido: no

Normal

Un valor booleano que es `true` si la instancia funciona con normalidad o `false` si la instancia se encuentra en un estado de error.

Tipo: Booleano

Obligatorio: no

Status

Estado de la instancia. Para una réplica `StatusType` de lectura, los valores pueden ser `replicating`, error, `stopped` o `terminated`.

Tipo: cadena

Requerido: no

StatusType

Actualmente, este valor es “`read replication`”.

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

DBSubnetGroup

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Información detallada sobre un grupo de subredes.

Contenido

> **Note**
>
> Los parámetros obligatorios se describen primero en la siguiente tabla.

DBSubnetGroupArn

El Nombre de recurso de Amazon (ARN) para el grupo de subred de base de datos.

Tipo: cadena

Requerido: no

DBSubnetGroupDescription

Proporciona la descripción del grupo de subred.

Tipo: cadena

Requerido: no

DBSubnetGroupName

El nombre del grupo de subred.

Tipo: cadena

Requerido: no

SubnetGroupStatus

Proporciona el estado del grupo de subred.

Tipo: cadena

Requerido: no

Subnets.Subnet.N

Información detallada sobre una o varias subredes dentro de un grupo de subredes.

Tipo: matriz de objetos Subnet

Obligatorio: no

SupportedNetworkTypes.member.N

El tipo de red del grupo de subredes de base de datos.

Valores válidos: `IPV4` | `DUAL`

Un `DBSubnetGroup` admite solamente el protocolo IPv4 o los protocolos IPv4 e IPv6 (DOBLE).

Tipo: matriz de cadenas

Obligatorio: no

VpcId

Proporciona el ID de la nube privada virtual (VPC) del grupo de subredes.

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

Endpoint

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Información de red para acceder a un clúster o a una instancia. Los programas cliente deben especificar un punto de conexión válido para acceder a estos recursos de Amazon DocumentDB.

Contenido

> **Note**
>
> Los parámetros obligatorios se describen primero en la siguiente tabla.

Address

Especifica la dirección DNS de la instancia.

Tipo: cadena

Requerido: no

HostedZoneId

Especifica el ID que Amazon Route 53 asigna al crear una zona alojada.

Tipo: cadena

Requerido: no

Port

Especifica el puerto en el que escucha el motor de la base de datos.

Tipo: entero

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- AWS SDK para C++

- AWS SDK para Java V2
- AWS SDK para Ruby V3

EngineDefaults

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Contiene el resultado de una invocación correcta de la operación `DescribeEngineDefaultClusterParameters`.

Contenido

> **Note**
>
> Los parámetros obligatorios se describen primero en la siguiente tabla.

DBParameterGroupFamily

El nombre de la familia del grupo de parámetros de clúster para la que devolver información de los parámetros del motor.

Tipo: cadena

Requerido: no

Marker

Un token de paginación opcional proporcionado por una solicitud anterior. Si se especifica este parámetro, la respuesta solo incluye registros más allá del marcador, hasta el valor especificado por `MaxRecords`.

Tipo: cadena

Requerido: no

Parameters.Parameter.N

Los parámetros de una familia de grupos de parámetros de clúster concreta.

Tipo: matriz de objetos Parameter

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

Event

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Información detallada sobre un evento.

Contenido

> **Note**
>
> Los parámetros obligatorios se describen primero en la siguiente tabla.

Date

Especifica la fecha y la hora del evento.

Tipo: marca temporal

Obligatorio: no

EventCategories.EventCategory.N

Especifica la categoría para el evento.

Tipo: matriz de cadenas

Obligatorio: no

Message

Proporciona el texto de este evento.

Tipo: cadena

Requerido: no

SourceArn

El Nombre de recurso de Amazon (ARN) para el evento.

Tipo: cadena

Requerido: no

SourceIdentifier

Proporciona el identificador del origen del evento.

Tipo: cadena

Requerido: no

SourceType

Especifica el tipo de origen para este evento.

Tipo: cadena

Valores válidos: `db-instance | db-parameter-group | db-security-group | db-snapshot | db-cluster | db-cluster-snapshot`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

EventCategoriesMap

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Un tipo de fuente de eventos, acompañado de uno o más nombres de categorías de eventos.

Contenido

> **Note**
>
> Los parámetros obligatorios se describen primero en la siguiente tabla.

EventCategories.EventCategory.N

Las categorías de eventos para el tipo de origen especificado.

Tipo: matriz de cadenas

Obligatorio: no

SourceType

El tipo de origen al que pertenecen las categorías devueltas.

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

EventSubscription

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Información detallada sobre un evento al que se ha suscrito.

Contenido

> **Note**
>
> Los parámetros obligatorios se describen primero en la siguiente tabla.

CustomerAwsId

La cuenta de cliente de AWS asociada a la suscripción a notificaciones de eventos de Amazon DocumentDB.

Tipo: cadena

Requerido: no

CustSubscriptionId

El ID de la suscripción a notificaciones de eventos de Amazon DocumentDB.

Tipo: cadena

Requerido: no

Enabled

Un valor booleano que indica si la suscripción está habilitada. Un valor de `true` indica que se ha activado la suscripción.

Tipo: Booleano

Obligatorio: no

EventCategoriesList.EventCategory.N

Una lista de categorías de eventos para la suscripción a notificaciones de eventos de Amazon DocumentDB.

Tipo: matriz de cadenas

Obligatorio: no

EventSubscriptionArn

El Nombre de recurso de Amazon (ARN) para la suscripción de eventos.

Tipo: cadena

Requerido: no

SnsTopicArn

El ARN del tema de la suscripción a notificaciones de eventos de Amazon DocumentDB.

Tipo: cadena

Requerido: no

SourceIdsList.SourceId.N

Una lista de ID de origen para la suscripción a notificaciones de eventos de Amazon DocumentDB.

Tipo: matriz de cadenas

Obligatorio: no

SourceType

El tipo de origen para la suscripción a notificaciones de eventos de Amazon DocumentDB.

Tipo: cadena

Requerido: no

Status

El estado de la suscripción a notificaciones de eventos de Amazon DocumentDB.

Restricciones:

Puede ser uno de los siguientes: `creating`, `modifying`, `deleting`, `active`, `no-permission`, `topic-not-exist`

El estado `no-permission` indica que Amazon DocumentDB ya no tiene permiso para publicar en el tema de SNS. El estado `topic-not-exist` indica que el tema se eliminó después de crear la suscripción.

Tipo: cadena

Requerido: no

SubscriptionCreationTime

La hora a la que se creó la suscripción a notificaciones de eventos de Amazon DocumentDB.

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

Filter

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Un conjunto de valores de filtro con nombre, que se utiliza para devolver una lista de resultados más específica. Puede usar un filtro que coincida con un conjunto de recursos según criterios específicos, como los ID.

No se admite el uso de comodines en los filtros.

Contenido

> **Note**
>
> Los parámetros obligatorios se describen primero en la siguiente tabla.

Name

El nombre del filtro. Los nombres de filtros distinguen entre mayúsculas y minúsculas.

Tipo: cadena

Obligatorio: sí

Values.Value.N

Uno o varios valores de filtros. Los valores de filtro distinguen entre mayúsculas y minúsculas.

Tipo: matriz de cadenas

Obligatorio: sí

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

GlobalCluster

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Tipo de datos que representa un clúster global de Amazon DocumentDB.

Contenido

> **Note**
>
> Los parámetros obligatorios se describen primero en la siguiente tabla.

DatabaseName

El nombre predeterminado de la base de datos del nuevo clúster global.

Tipo: cadena

Requerido: no

DeletionProtection

La configuración de protección contra eliminación para el nuevo clúster global.

Tipo: Booleano

Obligatorio: no

Engine

El motor de base de datos Amazon DocumentDB utilizado por el clúster global.

Tipo: cadena

Requerido: no

EngineVersion

Indica la versión del motor de base de datos.

Tipo: cadena

Requerido: no

GlobalClusterArn

El Nombre de recurso de Amazon (ARN) para el clúster global.

Tipo: cadena

Requerido: no

GlobalClusterIdentifier

Contiene un identificador de clúster global suministrado por el usuario. Este identificador es la clave única que identifica un clúster global.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 255 caracteres.

Patrón: `[A-Za-z][0-9A-Za-z-:._]*`

Obligatorio: no

GlobalClusterMembers.GlobalClusterMember.N

La lista de identificadores de clúster para los clústeres secundarios dentro del clúster global. Actualmente está limitada a un elemento.

Tipo: matriz de objetos GlobalClusterMember

Obligatorio: no

GlobalClusterResourceId

El identificador inmutable exclusivo de la región de Región de AWS para el clúster de la base de datos global. Este identificador se encuentra en las entradas de registro de AWS CloudTrail siempre que se accede a la clave maestra del cliente (CMK) de AWS KMS del clúster.

Tipo: cadena

Requerido: no

Status

Especifica el estado actual de este clúster global.

Tipo: cadena

Requerido: no

StorageEncrypted

Configuración de cifrado de almacenamiento para el clúster global.

Tipo: Booleano

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

GlobalClusterMember

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Estructura de datos con información sobre cualquier clúster primario y secundario asociado a un clúster global de Amazon DocumentDB.

Contenido

> **Note**
>
> Los parámetros obligatorios se describen primero en la siguiente tabla.

DBClusterArn

El Nombre de recurso de Amazon (ARN) para cada clúster de Amazon DocumentDB.

Tipo: cadena

Requerido: no

IsWriter

Especifica si el clúster de Amazon DocumentDB es el clúster primario (es decir, tiene capacidad de lectura y escritura) para el clúster global de Amazon DocumentDB al que está asociado.

Tipo: Booleano

Obligatorio: no

Readers.member.N

El Nombre de recurso de Amazon (ARN) para cada clúster secundario de solo lectura asociado al clúster global de Amazon DocumentDB.

Tipo: matriz de cadenas

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

OrderableDBInstanceOption

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Las opciones disponibles para una instancia.

Contenido

> **Note**
>
> Los parámetros obligatorios se describen primero en la siguiente tabla.

AvailabilityZones.AvailabilityZone.N

Una lista de zonas de disponibilidad para una instancia.

Tipo: matriz de objetos AvailabilityZone

Obligatorio: no

DBInstanceClass

La clase de instancia de una instancia.

Tipo: cadena

Requerido: no

Engine

El tipo de motor de una instancia.

Tipo: cadena

Requerido: no

EngineVersion

La versión de motor de una instancia.

Tipo: cadena

Requerido: no

LicenseModel

El modelo de licencia de una instancia.

Tipo: cadena

Requerido: no

StorageType

El tipo de almacenamiento que se va a asociar al clúster de base de datos

Tipo: cadena

Requerido: no

Vpc

Indica si una instancia es una nube privada virtual (VPC).

Tipo: Booleano

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- AWS SDK para C++
- AWS SDK para Java V2
- SDK de AWS para Ruby V3

Parameter

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Información detallada sobre un parámetro individual.

Contenido

> **Note**
>
> Los parámetros obligatorios se describen primero en la siguiente tabla.

AllowedValues

Especifica el rango de valores válido del parámetro.

Tipo: cadena

Requerido: no

ApplyMethod

Indica cuándo deben aplicarse actualizaciones de parámetros.

Tipo: cadena

Valores válidos: `immediate | pending-reboot`

Obligatorio: no

ApplyType

Especifica el tipo de parámetros específicos del motor.

Tipo: cadena

Requerido: no

DataType

Especifica el tipo de datos válidos para el parámetro.

Tipo: cadena

Requerido: no

Description

Proporciona una descripción del parámetro.

Tipo: cadena

Requerido: no

IsModifiable

Indica si el parámetro se puede modificar (`true`) o no (`false`). Algunos parámetros tienen implicaciones de seguridad u operativas que impiden que puedan cambiarse.

Tipo: Booleano

Obligatorio: no

MinimumEngineVersion

La versión del motor más antigua al que se puede aplicar el parámetro.

Tipo: cadena

Requerido: no

ParameterName

Especifica el nombre del parámetro.

Tipo: cadena

Requerido: no

ParameterValue

Especifica el valor del parámetro. Debe ser uno o más de los `AllowedValues` para los parámetros del clúster en formato CSV:

Los valores válidos son:

- `enabled`: el clúster acepta conexiones seguras mediante TLS, versión 1.0 a 1.3.
- `disabled`: el clúster no acepta conexiones seguras mediante TLS.
- `fips-140-3`: el clúster solo acepta conexiones seguras según los requisitos de la publicación 140-3 de las Normas Federales de Procesamiento de la Información (FIPS). Esto solamente se admite a partir de los clústeres de Amazon DocumentDB 5.0 (versión del motor

3.0.3727) en las siguientes regiones: ca-central-1, us-west-2, us-east-1, us-east-2, us-gov-east-1, us-gov-west-1.

- `tls1.2+`: el clúster acepta conexiones seguras mediante TLS, versión 1.2 y superiores. Solo se admite a partir de Amazon DocumentDB 4.0 (versión de motor 2.0.10980) y Amazon DocumentDB 5.0 (versión de motor 3.0.11051).
- `tls1.3+`: el clúster acepta conexiones seguras mediante TLS, versión 1.3 y superiores. Solo se admite a partir de Amazon DocumentDB 4.0 (versión de motor 2.0.10980) y Amazon DocumentDB 5.0 (versión de motor 3.0.11051).

Tipo: cadena

Requerido: no

Source

Indica el origen del valor del parámetro.

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

PendingCloudwatchLogsExports

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Una lista de los tipos de registro cuya configuración sigue pendiente. Estos tipos de registro están en proceso de activación o desactivación.

Contenido

> **Note**
>
> Los parámetros obligatorios se describen primero en la siguiente tabla.

LogTypesToDisable.member.N

Tipos de registro que están en proceso de habilitarse. Una vez habilitados, estos tipos de logs se exportan a Registros de Amazon CloudWatch.

Tipo: matriz de cadenas

Obligatorio: no

LogTypesToEnable.member.N

Tipos de registro que están en proceso de desactivación. Una vez desactivados, estos tipos de registro no se exportan a CloudWatch Logs.

Tipo: matriz de cadenas

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

PendingMaintenanceAction

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Proporciona información acerca de una acción de mantenimiento pendiente para un recurso.

Contenido

> **Note**
>
> Los parámetros obligatorios se describen primero en la siguiente tabla.

Action

El tipo de acción de mantenimiento pendiente disponible para el recurso.

Tipo: cadena

Requerido: no

AutoAppliedAfterDate

La fecha del periodo de mantenimiento cuando se aplica la acción. La acción de mantenimiento se aplica al recurso durante su primer periodo de mantenimiento después de esta fecha. Si se especifica esta fecha, se omite cualquier solicitud de alta `next-maintenance`.

Tipo: marca temporal

Obligatorio: no

CurrentApplyDate

La fecha de entrada en vigor en que se aplica la acción de mantenimiento pendiente al recurso.

Tipo: marca temporal

Obligatorio: no

Description

Una descripción que proporciona información más detallada sobre la acción de mantenimiento.

Tipo: cadena

Requerido: no

ForcedApplyDate

La fecha en que se aplica automáticamente la acción de mantenimiento. La acción de mantenimiento se aplica al recurso en esta fecha independientemente del periodo de mantenimiento para el recurso. Si se especifica esta fecha, se omite cualquier solicitud de alta `immediate`.

Tipo: marca temporal

Obligatorio: no

OptInStatus

Indica el tipo de solicitud de alta que se ha recibido para el recurso.

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK de para Ruby V3

PendingModifiedValues

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Uno o más ajustes modificados para una instancia. Estos ajustes modificados se han solicitado, pero aún no se han aplicado.

Contenido

> **Note**
>
> Los parámetros obligatorios se describen primero en la siguiente tabla.

AllocatedStorage

Contiene el tamaño nuevo de `AllocatedStorage` correspondiente a la instancia que se aplicará o que se está aplicando.

Tipo: entero

Obligatorio: no

BackupRetentionPeriod

Especifica el número de días pendientes durante los que se conservan las copias de seguridad automatizadas.

Tipo: entero

Obligatorio: no

CACertificateIdentifier

Especifica el identificador del certificado de CA para la instancia de base de datos.

Tipo: cadena

Requerido: no

DBInstanceClass

Contiene la nueva `DBInstanceClass` correspondiente a la instancia de base de datos que se aplicará o que se está aplicando.

Tipo: cadena

Requerido: no

DBInstanceIdentifier

Contiene la nueva `DBInstanceIdentifier` correspondiente a la instancia de base de datos que se aplicará o que se está aplicando.

Tipo: cadena

Requerido: no

DBSubnetGroupName

El nuevo grupo de subredes de la instancia.

Tipo: cadena

Requerido: no

EngineVersion

Indica la versión del motor de base de datos.

Tipo: cadena

Requerido: no

Iops

Especifica el nuevo valor de IOPS aprovisionadas correspondiente a la instancia de base de datos que se aplicará o que se está aplicando.

Tipo: entero

Obligatorio: no

LicenseModel

El modelo de licencia para la instancia.

Valores válidos: `license-included`, `bring-your-own-license`, `general-public-license`

Tipo: cadena

Requerido: no

MasterUserPassword

Contiene el cambio pendiente o actualmente en curso de las credenciales maestras para la instancia.

Tipo: cadena

Requerido: no

MultiAZ

Indica que la instancia Single-AZ va a cambiar a una implementación Multi-AZ.

Tipo: Booleano

Obligatorio: no

PendingCloudwatchLogsExports

Una lista de los tipos de registro cuya configuración sigue pendiente. Estos tipos de registro están en proceso de activación o desactivación.

Tipo: objeto PendingCloudwatchLogsExports

Obligatorio: no

Port

Especifica el puerto pendiente para la instancia.

Tipo: entero

Obligatorio: no

StorageType

Especifica el tipo de almacenamiento que se va a asociar con la instancia.

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

ResourcePendingMaintenanceActions

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Representa la salida de ApplyPendingMaintenanceAction.

Contenido

> **Note**
>
> Los parámetros obligatorios se describen primero en la siguiente tabla.

PendingMaintenanceActionDetails.PendingMaintenanceAction.N

Una lista que proporciona detalles sobre las acciones de mantenimiento pendientes para el recurso.

Tipo: matriz de objetos PendingMaintenanceAction

Obligatorio: no

ResourceIdentifier

El Nombre de recurso de Amazon (ARN) del recurso que tiene acciones de mantenimiento pendiente.

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK de para Ruby V3

ServerlessV2FeaturesSupport

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Especifica cualquier propiedad o límite de Amazon DocumentDB sin servidor que difiera entre las versiones del motor de Amazon DocumentDB. Puede probar los valores de este atributo cuando decide qué versión de Amazon DocumentDB va a utilizar en un clúster nuevo o actualizado. También puede recuperar la versión de un clúster existente y comprobar si esa versión admite determinadas características de Amazon DocumentDB sin servidor antes de intentar utilizarlas.

Contenido

> **Note**
>
> Los parámetros obligatorios se describen primero en la siguiente tabla.

MaxCapacity

El número máximo de unidades de capacidad de Amazon DocumentDB (DCU) para una instancia en un clúster de Amazon DocumentDB sin servidor. Puede especificar los valores de la DCU en incrementos de medio punto, como 32; 32,5; 33; etc.

Tipo: Doble

Obligatorio: no

MinCapacity

El número mínimo de unidades de capacidad de Amazon DocumentDB (DCU) para una instancia en un clúster de Amazon DocumentDB sin servidor. Puede especificar los valores de la DCU en incrementos de medio punto, como 8; 8,5; 9; etc.

Tipo: Doble

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

ServerlessV2ScalingConfiguration

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Establece la configuración de escalado del clúster de Amazon DocumentDB sin servidor.

Contenido

> **Note**
>
> Los parámetros obligatorios se describen primero en la siguiente tabla.

MaxCapacity

El número máximo de unidades de capacidad de Amazon DocumentDB (DCU) para una instancia en un clúster de Amazon DocumentDB sin servidor. Puede especificar los valores de la DCU en incrementos de medio punto, como 32; 32,5; 33; etc.

Tipo: Doble

Obligatorio: no

MinCapacity

El número mínimo de unidades de capacidad de Amazon DocumentDB (DCU) para una instancia en un clúster de Amazon DocumentDB sin servidor. Puede especificar los valores de la DCU en incrementos de medio punto, como 8; 8,5; 9; etc.

Tipo: Doble

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

ServerlessV2ScalingConfigurationInfo

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Recupera la configuración de escalado de un clúster de Amazon DocumentDB sin servidor.

Contenido

> **Note**
>
> Los parámetros obligatorios se describen primero en la siguiente tabla.

MaxCapacity

El número máximo de unidades de capacidad de Amazon DocumentDB (DCU) para una instancia en un clúster de Amazon DocumentDB sin servidor. Puede especificar los valores de la DCU en incrementos de medio punto, como 32; 32,5; 33; etc.

Tipo: Doble

Obligatorio: no

MinCapacity

El número mínimo de unidades de capacidad de Amazon DocumentDB (DCU) para una instancia en un clúster de Amazon DocumentDB sin servidor. Puede especificar los valores de la DCU en incrementos de medio punto, como 8; 8,5; 9; etc.

Tipo: Doble

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

Subnet

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Información detallada sobre una subred.

Contenido

> **Note**
>
> Los parámetros obligatorios se describen primero en la siguiente tabla.

SubnetAvailabilityZone

Especifica la Zona de Disponibilidad para la subred.

Tipo: objeto AvailabilityZone

Obligatorio: no

SubnetIdentifier

Especifica el identificador de la subred.

Tipo: cadena

Requerido: no

SubnetStatus

Especifica el estado de la subred.

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- AWS SDK para C++
- AWS SDK para Java V2

- AWS SDK para Ruby V3

Tag

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Metadatos asignados a un recurso de Amazon DocumentDB que consta de un par clave-valor.

Contenido

> **Note**
>
> Los parámetros obligatorios se describen primero en la siguiente tabla.

Key

El nombre obligatorio de la etiqueta. El valor de cadena puede tener una longitud de entre 1 y 128 caracteres Unicode y no puede llevar el prefijo “`aws:`“ ni “`rds:`“. La cadena puede contener únicamente el conjunto de letras, dígitos y espacio en blanco, “_”, “.”, “/”, “=”, “+”, “-” (Java regex: “^([\\p{L}\\p{Z}\\p{N}_.:/=+\\-]*)$”).

Tipo: cadena

Requerido: no

Value

Valor de cadena opcional de la etiqueta. El valor de cadena puede tener una longitud de entre 1 y 256 caracteres Unicode y no puede llevar el prefijo “`aws:`“ ni “`rds:`“. La cadena puede contener únicamente el conjunto de letras, dígitos y espacio en blanco, “_”, “.”, “/”, “=”, “+”, “-” (Java regex: “^([\\p{L}\\p{Z}\\p{N}_.:/=+\\-]*)$”).

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- AWS SDK para C++
- AWS SDK para Java V2

- AWS SDK para Ruby V3

UpgradeTarget

Servicio: Amazon DocumentDB (with MongoDB compatibility)

La versión del motor de base de datos a la que puede actualizarse una instancia.

Contenido

> **Note**
>
> Los parámetros obligatorios se describen primero en la siguiente tabla.

AutoUpgrade

Un valor que indica si la versión de destino se aplica a cualquier instancia de la base de datos de origen que se haya establecido `AutoMinorVersionUpgrade` en `true`.

Tipo: Booleano

Obligatorio: no

Description

La versión del motor de base de datos a la que puede actualizarse una instancia.

Tipo: cadena

Requerido: no

Engine

El nombre del motor de base de datos de destino de actualización.

Tipo: cadena

Requerido: no

EngineVersion

El número de versión del motor de base de datos de destino de actualización.

Tipo: cadena

Requerido: no

IsMajorVersionUpgrade

Un valor que indica si un motor de base de datos se actualiza a una versión principal.

Tipo: Booleano

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

VpcSecurityGroupMembership

Servicio: Amazon DocumentDB (with MongoDB compatibility)

Se utiliza como elemento de respuesta para consultas sobre la pertenencia a grupos de seguridad de la nube privada virtual (VPC).

Contenido

> **Note**
>
> Los parámetros obligatorios se describen primero en la siguiente tabla.

Status

El estado del grupo de seguridad de VPC.

Tipo: cadena

Requerido: no

VpcSecurityGroupId

El nombre del grupo de seguridad de VPC.

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

Amazon DocumentDB Elastic Clusters

Los siguientes tipos de datos son compatibles con los clústeres elásticos de Amazon DocumentDB:

- Cluster
- ClusterInList
- ClusterSnapshot
- ClusterSnapshotInList
- PendingMaintenanceActionDetails
- ResourcePendingMaintenanceAction
- Shard
- ValidationExceptionField

Cluster

Servicio: Amazon DocumentDB Elastic Clusters

Devuelve información sobre un clúster elástico específico.

Contenido

> **Note**
>
> Los parámetros obligatorios se describen primero en la siguiente tabla.

adminUserName

El nombre del administrador de los clústeres elásticos.

Tipo: cadena

Obligatorio: sí

authType

El tipo de autenticación del clúster elástico.

Tipo: cadena

Valores válidos: `PLAIN_TEXT | SECRET_ARN`

Obligatorio: sí

clusterArn

El identificador ARN del clúster elástico.

Tipo: cadena

Obligatorio: sí

clusterEndpoint

La URL que se usa para conectarse al clúster elástico.

Tipo: cadena

Obligatorio: sí

clusterName

El nombre del clúster elástico.

Tipo: cadena

Obligatorio: sí

createTime

La hora a la que se creó el clúster elástico, en tiempo universal coordinado (UTC).

Tipo: cadena

Obligatorio: sí

kmsKeyId

El identificador de clave de KMS que se debe utilizar para cifrar el clúster elástico.

Tipo: cadena

Obligatorio: sí

preferredMaintenanceWindow

El intervalo de tiempo semanal durante el cual puede llevarse a cabo el mantenimiento del sistema, en tiempo universal coordinado (UTC).

Formato: `ddd:hh24:mi-ddd:hh24:mi`

Tipo: cadena

Obligatorio: sí

shardCapacity

La cantidad de vCPU asignadas a cada partición de clúster elástico. El máximo es 64. Los valores permitidos son 2, 4, 8, 16, 32, 64.

Tipo: número entero

Obligatorio: sí

shardCount

El número de particiones asignadas al clúster elástico. El máximo es 32.

Tipo: número entero

Obligatorio: sí

status

Estado del clúster elástico.

Tipo: cadena

Valores válidos: `CREATING | ACTIVE | DELETING | UPDATING | VPC_ENDPOINT_LIMIT_EXCEEDED | IP_ADDRESS_LIMIT_EXCEEDED | INVALID_SECURITY_GROUP_ID | INVALID_SUBNET_ID | INACCESSIBLE_ENCRYPTION_CREDS | INACCESSIBLE_SECRET_ARN | INACCESSIBLE_VPC_ENDPOINT | INCOMPATIBLE_NETWORK | MERGING | MODIFYING | SPLITTING | COPYING | STARTING | STOPPING | STOPPED | MAINTENANCE | INACCESSIBLE_ENCRYPTION_CREDENTIALS_RECOVERABLE`

Obligatorio: sí

subnetIds

Los ID de subredes de Amazon EC2 para el clúster elástico.

Tipo: matriz de cadenas

Obligatorio: sí

vpcSecurityGroupIds

Una lista de grupos de seguridad de VPC de EC2 para asociar a este clúster elástico.

Tipo: matriz de cadenas

Obligatorio: sí

backupRetentionPeriod

El número de días durante los que se conservan las instantáneas de base de datos automáticas.

Tipo: entero

Obligatorio: no

preferredBackupWindow

El intervalo de tiempo diario durante el que se crean las copias de seguridad automatizadas si las copias de seguridad automatizadas están habilitadas según lo determina `backupRetentionPeriod`.

Tipo: cadena

Requerido: no

shardInstanceCount

El número de instancias de réplica que se aplica a todas las particiones del clúster. Un valor de `shardInstanceCount` igual a 1 significa que hay una instancia de escritura y las instancias adicionales son réplicas que se pueden usar para llevar a cabo lecturas y mejorar la disponibilidad.

Tipo: entero

Obligatorio: no

shards

El número total de particiones en el clúster.

Tipo: matriz de objetos Shard

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

ClusterInList

Servicio: Amazon DocumentDB Elastic Clusters

Lista de clústeres elásticos de Amazon DocumentDB.

Contenido

> **Note**
>
> Los parámetros obligatorios se describen primero en la siguiente tabla.

clusterArn

El identificador ARN del clúster elástico.

Tipo: cadena

Obligatorio: sí

clusterName

El nombre del clúster elástico.

Tipo: cadena

Obligatorio: sí

status

Estado del clúster elástico.

Tipo: cadena

Valores válidos: `CREATING | ACTIVE | DELETING | UPDATING | VPC_ENDPOINT_LIMIT_EXCEEDED | IP_ADDRESS_LIMIT_EXCEEDED | INVALID_SECURITY_GROUP_ID | INVALID_SUBNET_ID | INACCESSIBLE_ENCRYPTION_CREDS | INACCESSIBLE_SECRET_ARN | INACCESSIBLE_VPC_ENDPOINT | INCOMPATIBLE_NETWORK | MERGING | MODIFYING | SPLITTING | COPYING | STARTING | STOPPING | STOPPED | MAINTENANCE | INACCESSIBLE_ENCRYPTION_CREDENTIALS_RECOVERABLE`

Obligatorio: sí

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

ClusterSnapshot

Servicio: Amazon DocumentDB Elastic Clusters

Devuelve información sobre una instantánea específica del clúster elástico.

Contenido

> **Note**
>
> Los parámetros obligatorios se describen primero en la siguiente tabla.

adminUserName

El nombre del administrador de los clústeres elásticos.

Tipo: cadena

Obligatorio: sí

clusterArn

El identificador ARN del clúster elástico.

Tipo: cadena

Obligatorio: sí

clusterCreationTime

La hora a la que se creó el clúster elástico, en tiempo universal coordinado (UTC).

Tipo: cadena

Obligatorio: sí

kmsKeyId

El identificador de la clave de KMS es el Nombre de recurso de Amazon (ARN) de la clave de cifrado de KMS. Si está creando un clúster con la misma cuenta de Amazon a la que pertenece esta clave de cifrado de KMS, puede utilizar el alias de la clave de KMS en lugar del ARN como clave de cifrado de KMS. Si no se especifica una clave de cifrado, Amazon DocumentDB utiliza la clave de cifrado predeterminada que KMS crea para la cuenta. Su cuenta dispone de una clave de cifrado predeterminada diferente para cada región de Amazon.

Tipo: cadena

Obligatorio: sí

snapshotArn

El identificador ARN de la instantánea del clúster elástico.

Tipo: cadena

Obligatorio: sí

snapshotCreationTime

La hora a la que se creó la instantánea del clúster elástico en Tiempo Universal Coordinado (UTC).

Tipo: cadena

Obligatorio: sí

snapshotName

Nombre de la instantánea del clúster elástico.

Tipo: cadena

Obligatorio: sí

status

Estado de la instantánea del clúster elástico.

Tipo: cadena

Valores válidos: `CREATING | ACTIVE | DELETING | UPDATING | VPC_ENDPOINT_LIMIT_EXCEEDED | IP_ADDRESS_LIMIT_EXCEEDED | INVALID_SECURITY_GROUP_ID | INVALID_SUBNET_ID | INACCESSIBLE_ENCRYPTION_CREDS | INACCESSIBLE_SECRET_ARN | INACCESSIBLE_VPC_ENDPOINT | INCOMPATIBLE_NETWORK | MERGING | MODIFYING | SPLITTING | COPYING | STARTING | STOPPING | STOPPED | MAINTENANCE | INACCESSIBLE_ENCRYPTION_CREDENTIALS_RECOVERABLE`

Obligatorio: sí

subnetIds

Los ID de subredes de Amazon EC2 para el clúster elástico.

Tipo: matriz de cadenas

Obligatorio: sí

vpcSecurityGroupIds

Una lista de grupos de seguridad de VPC de EC2 para asociar al clúster elástico.

Tipo: matriz de cadenas

Obligatorio: sí

snapshotType

El tipo de instantáneas del clúster que se van a devolver. Puede especificar uno de los siguientes valores:

- `automated`: devuelve todas las instantáneas del clúster que Amazon DocumentDB haya creado automáticamente para su cuenta de AWS.
- `manual`: devuelve todas las instantáneas del clúster que haya creado manualmente para su cuenta de AWS.

Tipo: cadena

Valores válidos: `MANUAL | AUTOMATED`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

ClusterSnapshotInList

Servicio: Amazon DocumentDB Elastic Clusters

Lista de instantáneas de un clúster elástico.

Contenido

> **Note**
>
> Los parámetros obligatorios se describen primero en la siguiente tabla.

clusterArn

El identificador ARN del clúster elástico.

Tipo: cadena

Obligatorio: sí

snapshotArn

El identificador ARN de la instantánea del clúster elástico.

Tipo: cadena

Obligatorio: sí

snapshotCreationTime

La hora a la que se creó la instantánea del clúster elástico en Tiempo Universal Coordinado (UTC).

Tipo: cadena

Obligatorio: sí

snapshotName

Nombre de la instantánea del clúster elástico.

Tipo: cadena

Obligatorio: sí

status

Estado de la instantánea del clúster elástico.

Tipo: cadena

Valores válidos: `CREATING | ACTIVE | DELETING | UPDATING | VPC_ENDPOINT_LIMIT_EXCEEDED | IP_ADDRESS_LIMIT_EXCEEDED | INVALID_SECURITY_GROUP_ID | INVALID_SUBNET_ID | INACCESSIBLE_ENCRYPTION_CREDS | INACCESSIBLE_SECRET_ARN | INACCESSIBLE_VPC_ENDPOINT | INCOMPATIBLE_NETWORK | MERGING | MODIFYING | SPLITTING | COPYING | STARTING | STOPPING | STOPPED | MAINTENANCE | INACCESSIBLE_ENCRYPTION_CREDENTIALS_RECOVERABLE`

Obligatorio: sí

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

PendingMaintenanceActionDetails

Servicio: Amazon DocumentDB Elastic Clusters

Recupera los detalles de las acciones de mantenimiento pendientes.

Contenido

> **Note**
>
> Los parámetros obligatorios se describen primero en la siguiente tabla.

action

Muestra la acción específica de una acción de mantenimiento pendiente.

Tipo: cadena

Obligatorio: sí

autoAppliedAfterDate

Muestra la fecha del período de mantenimiento cuando se aplica la acción. La acción de mantenimiento se aplica al recurso durante su primer periodo de mantenimiento después de esta fecha. Si se especifica esta fecha, se omite cualquier solicitud de `optInType` de `NEXT_MAINTENANCE`.

Tipo: cadena

Requerido: no

currentApplyDate

Muestra la fecha de entrada en vigor en que se aplica la acción de mantenimiento pendiente al recurso.

Tipo: cadena

Requerido: no

description

Muestra una descripción que proporciona información más detallada sobre la acción de mantenimiento.

Tipo: cadena

Requerido: no

forcedApplyDate

Muestra la fecha en que se aplica automáticamente la acción de mantenimiento. La acción de mantenimiento se aplica al recurso en esta fecha independientemente del periodo de mantenimiento para el recurso. Si se especifica esta fecha, se omite cualquier solicitud de `optInType` de `IMMEDIATE`.

Tipo: cadena

Requerido: no

optInStatus

Muestra el tipo de solicitud de `optInType` que se ha recibido para el recurso.

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

ResourcePendingMaintenanceAction

Servicio: Amazon DocumentDB Elastic Clusters

Proporciona información acerca de una acción de mantenimiento pendiente para un recurso.

Contenido

> **Note**
>
> Los parámetros obligatorios se describen primero en la siguiente tabla.

pendingMaintenanceActionDetails

Proporciona información acerca de una acción de mantenimiento pendiente para un recurso.

Tipo: matriz de objetos PendingMaintenanceActionDetails

Obligatorio: no

resourceArn

El Nombre de recurso de Amazon (ARN) Amazon DocumentDB del recurso al que se aplica la acción de mantenimiento pendiente.

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

Shard

Servicio: Amazon DocumentDB Elastic Clusters

El nombre de la partición.

Contenido

> **Note**
>
> Los parámetros obligatorios se describen primero en la siguiente tabla.

createTime

La hora a la que se creó la partición, en tiempo universal coordinado (UTC).

Tipo: cadena

Obligatorio: sí

shardId

El ID de la partición.

Tipo: cadena

Obligatorio: sí

status

El estado actual de la partición.

Tipo: cadena

Valores válidos: `CREATING | ACTIVE | DELETING | UPDATING | VPC_ENDPOINT_LIMIT_EXCEEDED | IP_ADDRESS_LIMIT_EXCEEDED | INVALID_SECURITY_GROUP_ID | INVALID_SUBNET_ID | INACCESSIBLE_ENCRYPTION_CREDS | INACCESSIBLE_SECRET_ARN | INACCESSIBLE_VPC_ENDPOINT | INCOMPATIBLE_NETWORK | MERGING | MODIFYING | SPLITTING | COPYING | STARTING | STOPPING | STOPPED | MAINTENANCE | INACCESSIBLE_ENCRYPTION_CREDENTIALS_RECOVERABLE`

Obligatorio: sí

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

ValidationExceptionField

Servicio: Amazon DocumentDB Elastic Clusters

Un campo específico en el que se produjo una excepción de validación determinada.

Contenido

> **Note**
>
> Los parámetros obligatorios se describen primero en la siguiente tabla.

message

Un mensaje de error que describe la excepción de validación en este campo.

Tipo: cadena

Obligatorio: sí

name

El nombre del campo en el que se produjo la excepción de validación.

Tipo: cadena

Obligatorio: sí

Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un idioma específico, consulte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

Errores comunes

En esta sección, se enumeran los errores comunes a las acciones de la API de todos los servicios de AWS. En el caso de los errores específicos de una acción de la API de este servicio, consulte el tema de dicha acción de la API.

AccessDeniedException

No tiene acceso suficiente para realizar esta acción.

Código de estado HTTP: 400

IncompleteSignature

La firma de solicitud no se ajusta a los estándares de AWS.

Código de estado HTTP: 400

InternalFailure

El procesamiento de la solicitud ha devuelto un error debido a un error o una excepción desconocidos.

Código de estado HTTP: 500

InvalidAction

La acción u operación solicitada no es válida. Compruebe que la acción se ha escrito correctamente.

Código de estado HTTP: 400

InvalidClientTokenId

El certificado X.509 o el ID de clave de acceso de AWS proporcionado no existen en nuestros registros.

Código de estado HTTP: 403

NotAuthorized

No tiene permiso para realizar esta acción.

Código de estado HTTP: 400

OptInRequired

El ID de clave de acceso de AWS necesita una suscripción al servicio.

Código de estado HTTP: 403

RequestExpired

La solicitud llegó al servicio más de 15 minutos después de la marca de fecha en la solicitud o más de 15 minutos después de la fecha de vencimiento de la solicitud (por ejemplo, para las URL prefirmadas) o la marca de fecha de la solicitud corresponde a una hora futura en más de 15 minutos.

Código de estado HTTP: 400

ServiceUnavailable

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 503

ThrottlingException

La solicitud fue denegada debido a una limitación de la solicitud.

Código de estado HTTP: 400

ValidationError

La entrada no satisface las limitaciones que especifica un servicio de AWS.

Código de estado HTTP: 400

Parámetros comunes

La siguiente lista contiene los parámetros que utilizan todas las acciones para firmar solicitudes de Signature Version 4 con una cadena de consulta. Los parámetros específicos de acción se enumeran en el tema correspondiente a la acción. Para obtener más información sobre Signature Version 4, consulte Firma de solicitudes API de AWS en la Guía del usuario de IAM.

Action

Las acciones que se van a realizar.

Tipo: cadena

Obligatorio: sí

Version

La versión de la API para la que está escrita la solicitud, expresada en el formato AAAA-MM-DD.

Tipo: cadena

Obligatorio: sí

X-Amz-Algorithm

El algoritmo de hash que utilizó para crear la solicitud de firma.

Condición: especifique este parámetro cuando incluya información de autenticación en una cadena de consulta en lugar de en el encabezado de autorización HTTP.

Tipo: cadena

Valores válidos: `AWS4-HMAC-SHA256`

Obligatorio: condicional

X-Amz-Credential

El valor del ámbito de la credencial, que es una cadena que incluye la clave de acceso, la fecha, la región a la que se dirige, el servicio que solicita y una cadena de terminación (“aws4_request”). El valor se expresa en el siguiente formato: access_key/AAAAMMDD/region/service/aws4_request.

Para obtener más información, consulte Crear una solicitud API de AWS firmada en la Guía del usuario de IAM.

Condición: especifique este parámetro cuando incluya información de autenticación en una cadena de consulta en lugar de en el encabezado de autorización HTTP.

Tipo: cadena

Obligatorio: condicional

X-Amz-Date

La fecha utilizada para crear la firma. El formato debe ser ISO 8601 formato básico (AAAAMMDD‘T’HHMMSS‘Z’). Por ejemplo, la siguiente fecha y hora es un valor válido de X-Amz-Date para `20120325T120000Z`.

Condición: X-Amz-Date es opcional en todas las solicitudes; se puede utilizar para anular la fecha empleada a fin de firmar las solicitudes. Si el encabezado Date se especifica en el formato básico ISO 8601, no se requiere X-Amz-Date. Cuando se usa X-Amz-Date, siempre anula el valor del encabezado Date. Para obtener más información, consulte Elementos de una firma de solicitud API de AWS en la Guía del usuario de IAM.

Tipo: cadena

Obligatorio: condicional

X-Amz-Security-Token

El token de seguridad temporal que se obtuvo mediante una llamada a AWS Security Token Service (AWS STS). Para obtener una lista de servicios compatibles con las credenciales de seguridad temporales de AWS STS, consulte Servicios de AWS que funcionan con IAM en la Guía del usuario de IAM.

Condición: si utiliza credenciales de seguridad temporales de AWS STS, debe incluir el token de seguridad.

Tipo: cadena

Obligatorio: condicional

X-Amz-Signature

Especifica la firma codificada hexadecimal que se calculó a partir de la cadena que se va a firmar y la clave de firma derivada.

Condición: especifique este parámetro cuando incluya información de autenticación en una cadena de consulta en lugar de en el encabezado de autorización HTTP.

Tipo: cadena

Obligatorio: condicional

X-Amz-SignedHeaders

Especifica todos los encabezados HTTP que se incluyeron como parte de la solicitud canónica. Para obtener más información acerca de especificar encabezados firmados, consulte Crear una solicitud API de AWS firmada en la Guía del usuario de IAM.

Condición: especifique este parámetro cuando incluya información de autenticación en una cadena de consulta en lugar de en el encabezado de autorización HTTP.

Tipo: cadena

Obligatorio: condicional

Notas de la versión

Estas notas de versión describen las características, mejoras y correcciones de errores de Amazon DocumentDB por fecha de lanzamiento. Las notas de la versión incluyen actualizaciones para todas las versiones del motor Amazon DocumentDB a medida que se producen.

Para determinar la versión de parche actual del motor de Amazon DocumentDB, ejecute el siguiente comando:

```
db.runCommand({getEngineVersion: 1})
```

Si su clúster no está en la versión más reciente del motor, es probable que tenga disponibles tareas de mantenimiento pendientes que permitan actualizar el motor. Para obtener más información, consulte Mantenimiento de Amazon DocumentDB en la Guía para desarrolladores.

Puede filtrar nuevas características de Amazon DocumentDB en la página Novedades de Database. En Productos, elija Amazon DocumentDB. Luego, busque con palabras clave como **`elastic clusters`** o **`vector search`**.

Temas

- 08 de enero de 2026
- 11 de noviembre de 2025
- 22 de octubre de 2025
- 16 de octubre de 2025
- 13 de octubre de 2025
- 7 de octubre de 2025
- 26 de septiembre de 2025
- 15 de septiembre de 2025
- 29 de julio de 2025
- 28 de julio de 2025
- 18 de junio de 2025
- 8 de mayo de 2025
- 2 de abril de 2025

- 24 de marzo de 2025
- 6 de febrero de 2025
- 28 de enero de 2025
- 15 de enero de 2025
- 18 de diciembre de 2024
- 12 de noviembre de 2024
- 6 de noviembre de 2024
- 1 de noviembre de 2024
- 22 de octubre de 2024
- 18 de septiembre de 2024
- 17 de septiembre de 2024
- 22 de agosto de 2024
- 20 de agosto de 2024
- 8 de agosto de 2024
- 23 de julio de 2024
- 22 de julio de 2024
- 9 de julio de 2024
- 8 de julio de 2024
- 25 de junio de 2024
- 29 de mayo de 2024
- 3 de abril de 2024
- 22 de febrero de 2024
- 30 de enero de 2024
- 10 de enero de 2024
- 20 de diciembre de 2023
- 13 de diciembre de 2023
- 29 de noviembre de 2023
- 21 de noviembre de 2023
- 17 de noviembre de 2023

- 6 de noviembre de 2023
- 25 de septiembre de 2023
- 20 de septiembre de 2023
- 15 de septiembre de 2023
- 11 de septiembre de 2023
- 3 de agosto de 2023
- 13 de julio de 2023
- 7 de junio de 2023
- 10 de mayo de 2023
- 4 de abril de 2023
- 22 de marzo de 2023
- 1 de marzo de 2023
- 27 de febrero de 2023
- 2 de febrero de 2023
- 30 de noviembre de 2022
- 9 de agosto de 2022
- 25 de julio de 2022
- 27 de junio de 2022
- 29 de abril de 2022
- 7 de abril de 2022
- 16 de marzo de 2022
- 8 de febrero de 2022
- 24 de enero de 2022
- 21 de enero de 2022
- 25 de octubre de 2021
- 24 de junio de 2021
- 4 de mayo de 2021
- 15 de enero de 2021
- 9 de noviembre de 2020

- 30 de octubre de 2020
- 22 de septiembre de 2020
- 10 de julio de 2020
- 30 de junio de 2020

08 de enero de 2026

Nueva característica

Amazon DocumentDB ya está disponible en la región de Asia Pacífico (Yakarta). Para obtener más información, consulte esta entrada del blog.

11 de noviembre de 2025

Nuevas características

Amazon DocumentDB ahora ofrece una compatibilidad total de protocolos de cable con MongoDB 8.0. Amazon DocumentDB 8.0 mejora el rendimiento de las consultas y le permite crear aplicaciones de alto rendimiento a un costo menor.

Amazon DocumentDB 8.0 (parche del motor versión 4.0.4448)

- Se agregó soporte para los controladores de API de MongoDB 8.0.
- Se agregó compatibilidad con la versión 3 de Planner, que amplía las mejoras de rendimiento a los operadores de las etapas de agregación, además de admitir optimizaciones de la canalización de agregación y distintos comandos.
- Se agregó Support para la compresión basada en diccionarios a través del algoritmo de compresión Zstandard, lo que mejora la relación de compresión en 5 veces.
- Nuevas capacidades añadidas: Amazon DocumentDB 8.0 admite la intercalación y las vistas.
- Se agregó soporte para nuevas etapas y operadores de agregación: $replaceWith, $VectorSearch, $merge, $set, $unset, $bucket y 3 nuevos operadores de agregación $pow, $rand y $dateTrunc.
- Se agregó soporte para una nueva versión del índice de texto: el índice de texto v2 de Amazon DocumentDB 8.0 incorpora tokens adicionales, lo que mejora las capacidades de búsqueda de texto.

- Incluye mejoras en la búsqueda de vectores mediante la creación de índices vectoriales paralelos, lo que reduce el tiempo de creación de índices hasta 30 veces.

22 de octubre de 2025

Nuevas características

Amazon DocumentDB 5.0 (parche del motor versión 3.0.17983)

Amazon DocumentDB ahora es compatible con la última generación de instancias optimizadas para memoria con procesadores AWS Graviton4 basados en ARM, lo que proporciona un rendimiento hasta un 30% superior al de las instancias R6G. Para obtener más información, consulte Administración de clases de instancias en esta guía y este artículo del blog.

Amazon DocumentDB 5.0 (parche del motor versión 3.0.15902)

- Se agregó soporte para nombres de colección más largos (longitud del espacio de nombres de hasta 255 caracteres).
- Se introdujo un nuevo planificador de consultas (versión 2.0). Para obtener más información, consulte la sección Planificador de consultas v2 de esta guía.
- Se agregaron nuevos campos `collstats` para «» y MVCCIDStats «gcRuntimeStats» que proporcionan información sobre el estado general de la colección con respecto a la recolección de basura y las recolecciones antiguas.

Amazon DocumentDB 4.0 (parche del motor versión 2.0.11747)

Se agregaron nuevos campos `collstats` para «» y MVCCIDStats «gcRuntimeStats» que proporcionan información sobre el estado general de la colección con respecto a la recolección de basura y las recolecciones antiguas.

16 de octubre de 2025

Nueva característica

Amazon DocumentDB 5.0 (parche del motor versión 3.0.15902) y Amazon DocumentDB 4.0 (parche del motor versión 2.0.11747)

Amazon DocumentDB ahora admite el modo de doble pila (IPv4/IPv6) cuando el clúster se encuentra en una nube privada virtual (VPC).

Para obtener más información, consulte esta publicación del blog y Amazon VPC y Amazon DocumentDB en la Guía para desarrolladores de Amazon DocumentDB.

13 de octubre de 2025

Nueva característica

Amazon DocumentDB ahora es compatible con las instancias de R6G y T4G en la región de Asia-Pacífico (Hyderabad).

Para obtener más información, consulte Clases de instancias admitidas por región.

7 de octubre de 2025

Nueva característica

Amazon DocumentDB ahora está disponible en las siguientes regiones:

- Asia-Pacífico (Malasia)
- Asia-Pacífico (Osaka)
- Asia-Pacífico (Tailandia)
- México (centro)

Para obtener más información, consulte esta entrada del blog.

26 de septiembre de 2025

Nuevas características

Amazon DocumentDB ahora admite la copia y el uso compartido de instantáneas entre regiones y cuentas.

Para obtener más información, consulte Copiar instantáneas de un lado a otro Regiones de AWS y Uso compartido de instantáneas de clústeres de Amazon DocumentDB.

15 de septiembre de 2025

Correcciones de errores y otros cambios

Amazon DocumentDB 5.0 (parche del motor versión 3.0.17983)

Se corrigió un fallo del motor cuando las consultas incluyen una etapa posterior de `$replaceRoot` y `$lookup`.

29 de julio de 2025

Nuevas características

Amazon DocumentDB 5.0 (parche del motor versión 3.0.15902)

- Se agregó el soporte del operador de agregación de `$regexFindAll`.
- Se lanzaron métricas de sobrecarga de índices y sobrecarga basada en colecciones.
- Se agregaron CloudWatch métricas `AvailableMVCCIds` `LongestActiveGCRuntime` que proporcionan información sobre el estado general del clúster con respecto a la recolección de basura y la recolección de datos obsoletos.
- El `serverStatus` comando ahora incluye un campo «nvme_cache» que muestra el número de páginas escritas y no escritas en la NVMe caché en NVMe las instancias respaldadas.
- Se eliminó la limitación del número de campos para `$group` y `$project`.
- Se añadió soporte para los siguientes operadores de cadenas: `$trim`, `$rtrim`, `$ltrim`, `$regexFindAll`, `$replaceOne` y `$replaceAll`.
- Se añadió soporte para los siguientes operadores de matrices: `$first` y `$last`.
- Se añadió soporte para el siguiente operador de etapas: `$collStats`.

Amazon DocumentDB 4.0 (parche del motor versión 2.0.11747)

- Se lanzaron métricas de sobrecarga de índices y sobrecarga basada en colecciones.
- Se agregaron CloudWatch métricas `AvailableMVCCIds` `LongestActiveGCRuntime` que proporcionan información sobre el estado general del clúster con respecto a la recolección de basura y la recolección de datos obsoletos.
- Se añadió soporte para los siguientes operadores de cadenas: `$trim`, `$rtrim` y `$ltrim`.

- Se añadió soporte para el siguiente operador de etapas: `$collStats`.

Correcciones de errores y otros cambios

Amazon DocumentDB 5.0 (parche del motor versión 3.0.15902)

Se corrigió un problema durante la creación que afectaba las colecciones grandes.

Amazon DocumentDB 4.0 (parche del motor versión 2.0.11747)

Se corrigió un problema durante la creación que afectaba las colecciones grandes.

28 de julio de 2025

Nuevas características

Amazon DocumentDB 5.0 (parche del motor versión 3.0.14228)

Los clústeres basados en instancias de Amazon DocumentDB son compatibles con Amazon DocumentDB sin servidor, una configuración de escalado automático bajo demanda.

Para obtener más información, consulte Uso de Amazon DocumentDB sin servidor y esta entrada de novedades del blog.

18 de junio de 2025

Nueva característica

Amazon DocumentDB ahora está disponible en la región de Israel (Tel Aviv).

8 de mayo de 2025

Nueva característica

Amazon DocumentDB ahora está disponible en la región Europa (Estocolmo). Para obtener más información, consulte esta entrada del blog.

2 de abril de 2025

Correcciones de errores y otros cambios

Se corrigió un error en la creación de índices vectoriales con índices en segundo plano.

24 de marzo de 2025

Nueva característica

Amazon DocumentDB 5.0 (parche del motor versión 3.0.11800)

Se añadió soporte para los `postBatchResumeToken` en los flujos de cambios.

Para obtener más información, consulte Reanudación de un flujo de cambios con `postBatchResumeToken`.

6 de febrero de 2025

Nueva característica

Amazon DocumentDB ahora está integrado con. AWS Toolkit for Visual Studio Code Para obtener más información, consulte esta publicación de novedades del blog y consulte Uso de Amazon DocumentDB en el kit de herramientas en la Guía del usuario de AWS Toolkit for Visual Studio Code .

28 de enero de 2025

Nueva característica

Para una conectividad con un solo clic, Amazon DocumentDB ahora está integrado AWS CloudShell con cuatro clústeres elásticos y basados en instancias.

Para obtener más información, consulte cualquiera de los siguientes temas o todos ellos:

- Introducción a Amazon DocumentDB
- Introducción a los clústeres elásticos de Amazon DocumentDB
- Publicación de novedades del blog

- Entrada de la guía básica técnica

15 de enero de 2025

Nuevas características

Amazon DocumentDB 5.0 (parche del motor versión 3.0.11800)

Amazon DocumentDB ahora mantiene la disponibilidad de lectura mediante el reinicio de las instancias de escritura. Las instancias de lectura ahora seguirán atendiendo las solicitudes de lectura cuando se reinicie la instancia de escritura.

Correcciones de errores y otros cambios

Amazon DocumentDB 5.0 (parche del motor versión 3.0.11800)

- Se corrigió el comando `killOp` para gestionar un caso especial de inserciones masivas.
- Se mejoró el uso de memoria relacionado con las E/S de red en las instancias de Amazon DocumentDB.
- Se corrigió el comando `count` para consultas de filtro `$text`.

Amazon DocumentDB 4.0 (parche del motor versión 2.0.11096)

- Se corrigió el comando `killOp` para gestionar un caso especial de inserciones masivas.
- Se mejoró el uso de memoria relacionado con las E/S de red en las instancias de Amazon DocumentDB.

18 de diciembre de 2024

Nuevas características

Amazon DocumentDB 5.0 (versión de parche del motor 3.0.5721)

Los clústeres basados en instancias de Amazon DocumentDB ahora admiten instancias R6GD respaldadas NVMe.

Para obtener más información, consulte Instancias respaldadas por NVMe y esta entrada de novedades del blog.

12 de noviembre de 2024

Nuevas características

Los clústeres elásticos de Amazon DocumentDB son compatibles con los índices en segundo plano.

6 de noviembre de 2024

Nuevas características

Amazon DocumentDB 5.0 (parche del motor versión 3.0.11051)

- Se agregó soporte para las versiones mínimas de TLS `tls1.2+` y `tls1.3+` en el parámetro de clúster `tls`.
- Se habilitó la compatibilidad con los caracteres dólar ($) y punto (.) en los nombres de campo. Para conocer las diferencias funcionales, consulte Dólar($) y punto(.) en los nombres de campos.

Amazon DocumentDB 4.0 (parche del motor versión 2.0.10980)

- Se agregó soporte para las versiones mínimas de TLS `tls1.2+` y `tls1.3+` en el parámetro de clúster `tls`.

1 de noviembre de 2024

Nueva característica

Amazon DocumentDB ahora admite acciones de mantenimiento de clústeres elásticos. Para obtener más información, consulte Mantenimiento de clústeres elásticos de Amazon DocumentDB.

22 de octubre de 2024

Nueva característica

Amazon DocumentDB ahora admite métricas de rendimiento de la red de almacenamiento `StorageNetworkReceiveThroughput`, `StorageNetworkTransmitThroughput` y

`StorageNetworkThroughput`. Para obtener más información, consulte Evaluación del uso de instancias de Amazon DocumentDB con métricas CloudWatch .

18 de septiembre de 2024

Nueva característica

Amazon DocumentDB ahora está disponible en la región de África (Ciudad del Cabo). Para obtener más información, consulte esta entrada del blog.

Amazon DocumentDB ahora está disponible en la región Europa (España). Para obtener más información, consulte esta entrada del blog.

17 de septiembre de 2024

Nuevas características

Amazon DocumentDB 5.0 (versión de parche del motor 3.0.10696)

Amazon DocumentDB ahora admite la reconstrucción de índices con `reIndex` en `runCommand`. Para obtener más información, consulte Mantenimiento de índices mediante `reIndex`.

> **Note**
>
> `reIndex` solo es compatible con Amazon DocumentDB 5.0 (versión de parche del motor 3.0.10696 y posterior).

Correcciones de errores y otros cambios

Amazon DocumentDB 5.0 (versión de parche del motor 3.0.10696) y Amazon DocumentDB 4.0 (versión de parche del motor 2.0.10898)

- `$setOnInsert` ahora admite el campo `_id` durante las inserciones resultantes de las operaciones de actualización.
- Se corrigió un problema que impedía recuperar espacio de almacenamiento tras una actualización de una versión principal a Amazon DocumentDB 5.0.

22 de agosto de 2024

Nueva característica

Amazon DocumentDB 5.0 (todas las versiones de parche del motor) y Amazon DocumentDB 4.0 (versión de parche del motor 2.0.5704)

Los clústeres globales de Amazon DocumentDB ahora admiten transiciones de clústeres y conmutaciones por error de clústeres administradas. Para obtener más información, consulte Ejecución de una transición para un clúster global de Amazon DocumentDB y Ejecución de una conmutación por error administrada para un clúster global de Amazon DocumentDB.

> **Note**
>
> Las transiciones y conmutaciones por errores de clústeres globales solo son compatibles con Amazon DocumentDB 4.0 y 5.0.

20 de agosto de 2024

Nueva característica

Para Amazon DocumentDB 3.6 (versión mínima del parche del motor 1.0.208662), las actualizaciones del certificado TLS CA ya no requieren reiniciar el sistema. Para obtener más información, consulte Actualización de los certificados TLS de Amazon DocumentDB.

8 de agosto de 2024

Nueva característica

Los clústeres elásticos de Amazon DocumentDB ya están disponibles en las regiones Asia-Pacífico (Hong Kong), Canadá (centro) y Europa (París). Para obtener más información, consulte Disponibilidad regional para clústeres elásticos.

23 de julio de 2024

Nuevas características

Amazon DocumentDB 5.0 (versión de parche del motor 3.0.8126) y Amazon DocumentDB 4.0 (versión de parche del motor 2.0.10709)

- Se ha agregado compatibilidad con nombres de índice más largos (hasta 255 caracteres). Para obtener más información, consulte Restricciones en la nomenclatura
- Se ha duplicado el límite máximo de conexiones:

Tipo de instancia	Límite original	Nuevo límite
t3.medium	500	1 000
t4g.medium	500	1 000
r5.large	1700	3400
r5.xlarge	3500	7000
r5.2xlarge	7100	14200
r5.4xlarge	14200	28400
r5.8xlarge	28400	60000
r5.12xlarge	30000	60000
r5.16xlarge	30000	60000
r5.24xlarge	30000	60000
r6g.large	1700	3400
r6g.xlarge	3500	7000
r6g.2xlarge	7100	14200
r6g.4xlarge	14200	28400

Tipo de instancia	Límite original	Nuevo límite
r6g.8xlarge	28400	60000
r6g.12xlarge	30000	60000
r6g.16xlarge	30000	60000

Para obtener más información, consulte Límites de instancias.

Correcciones de errores y otros cambios

Amazon DocumentDB 5.0 (versión de parche del motor 3.0.8126)

Se ha mejorado la lógica para la sincronización de `CurrentTime` y `ResumeToken` para el flujo de cambios en los lectores.

22 de julio de 2024

Nuevas características

Amazon DocumentDB 5.0 (versión de parche del motor 3.0.6742)

- Se ha agregado compatibilidad con el filtrado de auditoría DML. Ahora puede configurar las condiciones de filtrado para filtrar los registros de auditoría de DML en función de sus requisitos específicos en lugar de registrar todas las consultas de DML. Para obtener más información, consulte Filtrado de eventos de auditoría de DML.
- Se ha agregado compatibilidad en la compresión de documentos para lo siguiente:
  - Establecimiento de un umbral de compresión mínimo
  - Habilitación de la compresión de las colecciones existentes (aplicable a los documentos nuevos)
  - Permiso para la opción de compresión predeterminada en el nivel de clúster

  Para obtener más información, consulte Gestión de la compresión de documentos a nivel de colección.
- Se ha agregado compatibilidad para consumir flujos de cambios en las instancias de lectura. Para obtener más información, consulte Uso de flujos de cambios en instancias secundarias.

Amazon DocumentDB 4.0 (versión de parche del motor 2.0.10593)

- Se ha agregado compatibilidad con el filtrado de auditoría DML. Ahora puede configurar las condiciones de filtrado para filtrar los registros de auditoría de DML en función de sus requisitos específicos en lugar de registrar todas las consultas de DML. Para obtener más información, consulte Filtrado de eventos de auditoría de DML.

Amazon DocumentDB 3.6 (versión de parche del motor 1.0.208662)

Se han eliminado las limitaciones de índice en las instancias db.r5.* y db.r6.* en la MVU de Amazon DocumentDB. Para obtener más información, consulte Requisitos previos y limitaciones de la MVU.

Correcciones de errores y otros cambios

Amazon DocumentDB 3.6 (versión de parche del motor 1.0.208662)

Amazon DocumentDB ahora reconoce -NaN como un token JSON válido.

9 de julio de 2024

Nueva característica

Para Amazon DocumentDB 4.0 (versión mínima del parche del motor 2.0.10179) y 5.0 (versión mínima del parche del motor 3.0.4780), las actualizaciones del certificado TLS CA ya no requieren reiniciar el sistema. Para obtener más información, consulte Actualización de los certificados TLS de Amazon DocumentDB.

8 de julio de 2024

Nueva característica

Los clústeres elásticos de Amazon DocumentDB ahora están disponibles en la región Europa (Milán). Para obtener más información, consulte Disponibilidad regional para clústeres elásticos.

25 de junio de 2024

Nueva característica

La autenticación con AWS IAM ARNs está disponible en los clústeres 5.0 basados en instancias de Amazon DocumentDB en todas las regiones compatibles. Para obtener más información, consulte Autenticación mediante la identidad de IAM.

29 de mayo de 2024

Nuevas características

Amazon DocumentDB 5.0 (versión de parche del motor 3.0.6742)

- Se ha agregado compatibilidad para los operadores `$regexMatch` y `$regexFind`.
- Se ha agregado compatibilidad para garantizar una precisión total en los registros de auditoría cuando se abordan números enteros grandes. Los registros de auditoría ahora mantienen la representación numérica exacta de todos los números, lo que evita cualquier pérdida de precisión.

Amazon DocumentDB 4.0 (versión de parche del motor 2.0.10593)

- Se ha agregado compatibilidad para garantizar una precisión total en los registros de auditoría cuando se abordan números enteros grandes. Los registros de auditoría ahora mantienen la representación numérica exacta de todos los números, lo que evita cualquier pérdida de precisión.

3 de abril de 2024

Amazon DocumentDB ahora está disponible en la región de Medio Oriente (EAU). Para obtener más información, consulte esta entrada del blog.

Nuevas características

Amazon DocumentDB 5.0 (versión de parche del motor 3.0.5721)

- Se ha agregado compatibilidad con `bypassDocumentValidation` y un mensaje de error detallado para `$jsonSchema`. Para obtener más información acerca de `bypassDocumentValidation`, consulte bypassDocumentValidation.

- Se ha agregado compatibilidad con `$expr`.
- Se ha agregado compatibilidad con uniones no correlacionadas en `$lookup`.
- Se ha agregado compatibilidad para retener las reglas de validación en la etapa de agregación de `$out`.

Amazon DocumentDB 4.0 (versión de parche del motor 2.0.10392)

- Se ha agregado compatibilidad con `bypassDocumentValidation` para `$jsonSchema`. Para obtener más información acerca de `bypassDocumentValidation`, consulte bypassDocumentValidation.
- Se ha agregado compatibilidad con `$expr`.
- Se ha agregado compatibilidad con uniones no correlacionadas en `$lookup`.
- Se ha agregado compatibilidad para retener las reglas de validación en la etapa de agregación de `$out`.

Correcciones de errores y otros cambios

- Se ha corregido un error al invocar `db.coll.stats()` en la versión 1.7 y posteriores del intérprete de comandos de mongo.
- Se ha corregido un problema de pérdida de memoria en las consultas de flujo de cambios que contenían `$regex` como parte de la misma canalización de agregación.

22 de febrero de 2024

Nuevas características

Clústeres elásticos de Amazon DocumentDB

Los clústeres elásticos de Amazon DocumentDB ahora admiten las siguientes características:

- Réplicas legibles de instancias con particiones secundarias: para obtener más información, consulte el paso 5b de Paso 1: crear un clúster elástico.
- Inicio o detención de un clúster: para obtener más información, consulte Detención e inicio de un clúster elástico de Amazon DocumentDB.

- Instancias con particiones configurables: para obtener más información, consulte el paso 5b de Paso 1: crear un clúster elástico.
- Copias de seguridad automáticas para instantáneas: para obtener más información, consulte Administración de una copia de seguridad automática de una instantánea de un clúster elástico.
- Copia de instantáneas: para obtener más información, consulte Copia de una instantánea de un clúster elástico.

30 de enero de 2024

Nuevas características

Clústeres elásticos de Amazon DocumentDB

Los clústeres elásticos de Amazon DocumentDB ahora están disponibles en las siguientes regiones:

- Asia-Pacífico (Mumbai)
- Asia-Pacífico (Seúl)
- América del Sur (São Paulo)
- Europa (Londres)

Para obtener más información, consulte Disponibilidad en regiones y versiones de clústeres elásticos.

Clústeres globales de Amazon DocumentDB

Los clústeres globales ahora están disponibles en ambas AWS GovCloud (US) regiones: AWS GovCloud (EE. UU. este) y (EE. UU. oeste). AWS GovCloud

10 de enero de 2024

Nuevas características

Amazon DocumentDB 5.0 (versiones de parche del motor 3.0.4574, 3.0.4780 y 3.0.4960)

- Se ha agregado compatibilidad para los índices vectoriales HNSW. Para obtener más información, consulte Búsqueda vectorial para Amazon DocumentDB.

- Se ha agregado compatibilidad para índices parciales. Para obtener más información, consulte Índice parcial.
- Se ha agregado compatibilidad para el tiempo de ejecución de GC en una colección dentro del comando `currentOp`.
- Se ha agregado compatibilidad con índices de texto para la búsqueda de texto nativo en Amazon DocumentDB. Para obtener más información, consulte Búsquedas de texto con Amazon DocumentDB.
- Se ha agregado compatibilidad con las palabras clave de esquema `$jsonSchema` `type`, `allOf`, `oneOf`, `anyOf`, `not`, `maxItems`, `minItems`, `maxProperties`, `minProperties`, `pattern`, `patternProperties`, `multipleOf`, `dependencies` y `uniqueItems`.

  Para obtener más información, consulte Cómo utilizar la validación de esquemas JSON.
- Se ha agregado compatibilidad para los operadores aritméticos `$ceil`, `$floor`, `$ln`, `$log`, `$log10`, `$sqrt` y `$exp`.

  Para obtener más información, consulte Operadores aritméticos.
- Se ha agregado compatibilidad para el operador de expresión condicional `$switch`.
- Se ha agregado compatibilidad para compilaciones de índices de vector `IVFFLAT` en paralelo. La documentación se ha actualizado al eliminar la limitación de compilaciones de índices vectoriales `IVFFLAT` paralelos de la guía para desarrolladores.

Amazon DocumentDB 4.0 (versiones de parche del motor 2.0.10124, 2.0.10179 y 2.0.10221)

- Se ha agregado compatibilidad para el tiempo de ejecución de GC en una colección dentro del comando `currentOp`.
- Se ha agregado compatibilidad con las palabras clave de esquema `$jsonSchema` `type`, `allOf`, `oneOf`, `anyOf`, `not`, `maxItems`, `minItems`, `maxProperties`, `minProperties`, `pattern`, `patternProperties`, `multipleOf`, `dependencies` y `uniqueItems`.

  Para obtener más información, consulte Cómo utilizar la validación de esquemas JSON.
- Se ha agregado compatibilidad para los operadores aritméticos `$ceil`, `$floor`, `$ln`, `$log`, `$log10`, `$sqrt` y `$exp`.

  Para obtener más información, consulte Operadores aritméticos.
- Se ha agregado compatibilidad para el operador de expresión condicional `$switch`.

Correcciones de errores y otros cambios

- Se ha agregado la funcionalidad que no distingue entre mayúsculas y minúsculas para invocar `db.runCommand("dbstats")`. Los clientes de Amazon DocumentDB 5.0 y 4.0 con versiones de parches del motor anteriores a 3.0.4960 o 2.0.10221 deben aplicar estos últimos parches del motor.
- Se ha corregido un error al invocar `db.coll.stats()` en la versión 1.7 y posteriores del intérprete de comandos de mongo. La documentación se ha actualizado al eliminar el consejo de solución de problemas `db.coll.stats()` del intérprete de comandos de mongo de la guía para desarrolladores.

20 de diciembre de 2023

Otros cambios

Se ha habilitado la compatibilidad para las actualizaciones locales de las versiones principales en Amazon DocumentDB 3.6 y 4.0. Para obtener más información, consulte Actualización local de la versión principal Amazon DocumentDB.

13 de diciembre de 2023

Nuevas características

Se ha añadido soporte para la conectividad con un solo clic. EC2 Para obtener más información, consulte Connect mediante Amazon EC2.

29 de noviembre de 2023

Amazon DocumentDB 5.0 (versión de parche del motor 3.0.3727)

Nuevas características

Se ha agregado compatibilidad para la búsqueda vectorial. Para obtener más información, consulte esta publicación de blog y visite Búsqueda vectorial para Amazon DocumentDB en la Guía para desarrolladores de Amazon DocumentDB.

21 de noviembre de 2023

Amazon DocumentDB 5.0 (versión de parche del motor 3.0.3727)

Nuevas características

Se ha agregado compatibilidad para almacenamiento optimizado para E/S. Para obtener más información, consulte Configuraciones de almacenamiento en clústeres de Amazon DocumentDB en la Guía para desarrolladores de Amazon DocumentDB.

Se agregó la integración para el aprendizaje automático sin código con SageMaker Canvas. Para obtener más información, consulte Aprendizaje automático sin código con Amazon SageMaker AI Canvas en la Guía para desarrolladores de Amazon DocumentDB.

17 de noviembre de 2023

Nuevas características

Amazon DocumentDB ya está disponible en la región AWS GovCloud (EE.UU. Este). Para obtener más información, consulte esta entrada del blog.

Correcciones de errores y otros cambios

Amazon DocumentDB 3.6 (versión de parche del motor 1.0.208570)

Los nombres de variables locales definidos por el usuario ahora admiten "_" (guion bajo) para operadores de proyección como `$let` y `$filter`.

6 de noviembre de 2023

Amazon DocumentDB 5.0 (versión de parche del motor 3.0.3727) y 4.0 (versión de parche del motor 2.0.9876)

Nuevas características

- Se agregó compatibilidad con las palabras clave de esquema `$jsonSchema` `maxLength`, `minLength`, `maximum`, `minimum`, `exclusiveMaximum`, `exclusiveMinimum`, `items` y `additionalItems`.

Tenga en cuenta que la validación de esquemas JSON solo es compatible con clústeres basados en instancias.

- Se agregó soporte para el operador de canalización de agregación `$convert` y sus operadores derivados de forma abreviada `$toBool`, `$toInt`, `$toLong`, `$toDouble`, `$toString`, `$toDecimal`, `$toObjectId` y `$toDate`.
- Se agregó compatibilidad con los operadores de expresiones de conjuntos `$setDifference`, `$anyElementTrue`, y `$allElementTrue`.

Correcciones de errores y otros cambios

Se ha corregido un error que provocaba que no se mostrara de `-NaN` a `NaN` una actualización del flujo de cambios.

25 de septiembre de 2023

Nuevas características

Amazon DocumentDB ya está disponible en la región Asia-Pacífico (Hong Kong). Para obtener más información, consulte esta entrada del blog.

20 de septiembre de 2023

Nuevas características

Se agregó compatibilidad para las actualizaciones de versiones principales en el lugar en Amazon DocumentDB 3.6 y 4.0. Para obtener más información, consulte Actualización local de la versión principal Amazon DocumentDB.

15 de septiembre de 2023

Nuevas características

Amazon DocumentDB 5.0 (versión de parche del motor 3.0.3140) y 4.0 (versión de parche del motor 2.0.9686)

Se ha agregado compatibilidad para el validador de esquemas $jsonSchema solo en clústeres basados en instancias. Para obtener más información, consulte Cómo utilizar la validación de esquemas JSON.

11 de septiembre de 2023

Nuevas características

Amazon DocumentDB ya está disponible en la región de Asia-Pacífico (Hyderabad). Para obtener más información, consulte esta entrada del blog.

3 de agosto de 2023

Nuevas características

Clústeres elásticos de Amazon DocumentDB

- Los clústeres elásticos de Amazon DocumentDB ahora admiten las siguientes operaciones:
  - `top`
  - `collStats`
  - `hint`
  - `dataSize`

  Consulte APIsMongoDB, operaciones y tipos de datos compatibles en Amazon DocumentDB para ver una lista completa de comandos y operaciones admitidos.
- Ahora se admiten los índices de tiempo de vida (TTL, Tiempo de vida).
- Las `hints` de índices son compatibles con las expresiones de índice.

13 de julio de 2023

Nuevas características

Amazon DocumentDB 5.0 (versión de parche del motor 3.0.1948)

- Se ha agregado compatibilidad con la compresión de documentos.
- Se agregó compatibilidad para compilaciones de índices en paralelo.

- Se agregó compatibilidad para el estado de compilación del índice.

Amazon DocumentDB 4.0 (versión de parche del motor 2.0.9259)

- Se agregó compatibilidad para compilaciones de índices en paralelo.

Correcciones de errores y otros cambios

Amazon DocumentDB 5.0 (versión de parche del motor 3.0.1948)

- Se ha corregido un problema de autenticación con `createCollection` los clústeres elásticos de Amazon DocumentDB cuando los usuarios no tienen acceso a las colecciones del sistema.
- Se solucionó el problema por el que las instancias de la región secundaria no podían usar los mismos nombres de instancia de la región principal.

Amazon DocumentDB 4.0 (versión de parche del motor 2.0.9259)

- Se dejó de añadir consultas de monitoreo interna a los registros de auditoría.

7 de junio de 2023

Correcciones de errores y otros cambios

Amazon DocumentDB 5.0

- Las instancias r5 y t3.medium ya son compatibles con Amazon DocumentDB 5.0.
- `engineVersion`la opción predeterminada está `5.0.0` en el AWS SDK AWS CLI, y. CloudFormation

10 de mayo de 2023

Correcciones de errores y otros cambios

Amazon DocumentDB 5.0 (versión de parche del motor 3.0.1361)

- Incorpora compatibilidad con los `ignoreunknownindexoptions` en la consola de createIndex.

- Se dejó de añadir consultas de monitoreo interna a los registros de auditoría.
- Los nombres de variables locales definidos por el usuario ahora admiten “_” (guion bajo) para operadores de proyección como `$let` y `$filter`.

4 de abril de 2023

Correcciones de errores y otros cambios

Amazon DocumentDB 4.0 (versión de parche del motor 2.0.8934)

- Se solucionó el problema con la auditoría de DML cuando estaba habilitada durante una carga de trabajo continua.
- Se solucionó el problema con la auditoría de DML que provocaba que a los comandos agregados con una sugerencia se les pasara un valor de cadena.
- Se solucionó el problema por el que el comando `listCollections` no funcionaba cuando los usuarios con el rol readwriteanydatabase tenían las opciones AuthorizedCollections y NameOnly configuradas en true.
- Se solucionó el problema que impedía analizar correctamente la cadena numérica del nombre de un campo.
- Cancele los cursores de larga duración cuando afecten a la recopilación de elementos no utilizados.
- Los nombres de variables locales definidos por el usuario ahora admiten “_” (guion bajo) para operadores de proyección como `$let` y `$filter`.

22 de marzo de 2023

Nuevas características

Los clústeres elásticos de Amazon DocumentDB ya están disponibles en las regiones Asia-Pacífico (Singapur), Asia Pacífico (Sídney) y Asia Pacífico (Tokio). Para obtener más información, consulte Disponibilidad en regiones y versiones de clústeres elásticos.

1 de marzo de 2023

Nuevas características

Amazon DocumentDB 5.0 (versión de parche del motor 3.0.775)

- Se ha presentado Amazon DocumentDB 5.0
  - Compatibilidad con MongoDB 5.0 (soporte para los controladores API de MongoDB 5.0)
  - Compatibilidad con el cifrado a nivel de campo (FLE) del lado del cliente. Ahora puede cifrar los campos del lado del cliente antes de escribir los datos en el clúster de Amazon DocumentDB. Para obtener más información, consulte Cifrado a nivel de campo del lado del cliente
  - Nuevos operadores de agregación: `$dateAdd`, `$dateSubtract`
- Se aumentó el límite de almacenamiento a 128 TiB para los clústeres de Amazon DocumentDB basados en instancias y para los clústeres elásticos basados en particiones.
- Amazon DocumentDB 5.0 ahora admite escaneos de índices con el operador `$elemMatch` en el primer nivel de anidación. Los escaneos de índices se admiten cuando el filtro para solo consultas tiene un nivel de filtro de `$elemMatch` y la consulta `$elemMatch` anidada no admite el escaneo de índices.

  Forma de consulta que admite el escaneo de índices:

  ```
  db.foo.find( { "a": {$elemMatch: { "b": "xyz", "c": "abc"} } })
  ```

  Forma de consulta que no admite el escaneo de índices:

  ```
  db.foo.find( { "a": {$elemMatch: { "b": {$elemMatch: { "d": "xyz", "e":
   "abc"} }} } })
  ```

27 de febrero de 2023

Correcciones de errores y otros cambios

Amazon DocumentDB 4.0

Se agregó soporte para AWS Lambda. Para obtener más información, consulte Uso AWS Lambda con flujos de cambios.

2 de febrero de 2023

Correcciones de errores y otros cambios

Amazon DocumentDB 3.6 (versión de parche del motor 1.0.208432)

- Se solucionó el problema con la auditoría de DML cuando estaba habilitada durante una carga de trabajo continua.
- Se solucionó el problema con la auditoría de DML que provocaba que a los comandos agregados con una sugerencia se les pasara un valor de cadena.
- Se solucionó el problema por el que el comando `listCollections` no funcionaba cuando los usuarios con el rol readwriteanydatabase tenían las opciones AuthorizedCollections y NameOnly configuradas en true.
- Se solucionó el problema que impedía analizar correctamente la cadena numérica del nombre de un campo.
- Cancele los cursores de larga duración cuando afecten a la recopilación de elementos no utilizados.

30 de noviembre de 2022

Nuevas características

Clústeres elásticos de Amazon DocumentDB

Los clústeres elásticos de Amazon DocumentDB son un nuevo tipo de clúster de Amazon DocumentDB que permite a los usuarios aprovechar la fragmentación de MongoDB para escalar su clúster. APIs Los clústeres elásticos gestionan prácticamente cualquier cantidad de lecturas y escrituras con petabytes de capacidad de almacenamiento mediante la distribución de los datos y computación entre varios volúmenes e instancias de procesamiento subyacentes. Para obtener más información, consulte Uso de clústeres elásticos de Amazon DocumentDB.

9 de agosto de 2022

Nuevas características

Amazon DocumentDB 3.6 (versión de parche del motor 1.0.208152) y 4.0

- Se agregó soporte para el tipo de datos Decimal128. El Decimal128 es un tipo de datos BSON compatible con todas las regiones en las que DocumentDB está disponible.

  Para obtener más información, consulte Data Types.

- Se ha añadido compatibilidad con la auditoría de consultas de DML con Amazon CloudWatch Logs. Ahora Amazon DocumentDB puede registrar eventos del lenguaje de manipulación de datos (DML) y eventos del lenguaje de definición de datos (DDL) en Amazon Logs. CloudWatch

  Para obtener más información, consulte esta entrada del blog.

Correcciones de errores y otros cambios

Amazon DocumentDB 3.6 (versión de parche del motor 1.0.208152) y 4.0

- Ahora puede cambiar su propia contraseña por una contraseña propia con privilegios `changeOwnPassword`.

25 de julio de 2022

Nuevas características

Amazon DocumentDB 4.0

Ahora puede crear clústeres más rápido con la posibilidad de crear clones que usen el mismo volumen de clúster de DocumentDB y tengan los mismos datos que el clúster original. Para obtener más información, consulte Administración de clústeres de Amazon DocumentDB.

27 de junio de 2022

Nuevas características

Amazon DocumentDB 4.0 (versión de parche del motor 2.0.7509)

Amazon DocumentDB cambia el tamaño de la base de datos de forma dinámica en función de los patrones de uso. Añadir más datos aumenta el espacio hasta 64 Tebibytes (TiB) y eliminar datos reduce el espacio asignado.

29 de abril de 2022

Nuevas características

Amazon DocumentDB ya está disponible en la región China (Pekín). Para obtener más información, consulte esta entrada del blog.

7 de abril de 2022

Nuevas características

Amazon DocumentDB 3.6 (versiones de parche del motor 1.0.207836 y 1.0.208015) y 4.0 (versiones de parche del motor 2.0.6142 y 2.0.6948)

Amazon DocumentDB Performance Insights ya está en vista previa. Ahora puede almacenar siete días del historial de rendimiento en un período continuo sin costo adicional. Para obtener más información, consulte Supervisión con información sobre rendimiento.

16 de marzo de 2022

Nuevas características

Amazon DocumentDB ahora está disponible en la región Europa (Milán). Para obtener más información, consulte esta entrada del blog.

8 de febrero de 2022

Nuevas características

Las instancias R6g y T4g de Amazon DocumentDB ya están disponibles en Asia Pacífico, Sudamérica y Europa. Para obtener más información, consulte esta entrada del blog.

24 de enero de 2022

Nuevas características

Amazon DocumentDB 3.6 (versión de parche del motor 1.0.207684) y 4.0 (versión de parche del motor 2.0.5170)

- Amazon DocumentDB ahora ofrece una prueba gratuita. Para obtener más información, consulte la página de prueba gratuita de Amazon DocumentDB.
- Ahora puede utilizar funciones mejoradas con las consultas geoespaciales, incluidas las siguientes: APIs
  - `$geoWithin`
  - `$geoIntersects`
- Se ha agregado compatibilidad con los siguientes operadores de MongoDB:
  - `$mergeObjects`
  - `$reduce`

  Para obtener más información, consulte Consulta de datos geoespaciales con Amazon DocumentDB.

21 de enero de 2022

Nuevas características

Amazon DocumentDB 4.0 (versión de parche del motor 2.0.5706)

- Ahora se admiten las instancias Graviton2 (r6g.large, r6g.2xlarge, r6g.4xlarge, r6g.8xlarge, r6g.12xlarge, r6g.16xlarge y t4g.medium) de Amazon DocumentDB.

Amazon DocumentDB 3.6 (versión de parche del motor 1.0.207781) y 4.0 (versión de parche del motor 2.0.5706)

- Se agregó soporte para los siguientes MongoDB APIs:
  - `$reduce`
  - `$mergeObjects`
  - `$geoWithin`
  - `$geoIntersects`

25 de octubre de 2021

Nuevas características

Amazon DocumentDB 3.6 (versión de parche del motor 1.0.207780) y 4.0 (versión de parche del motor 2.0.5704)

- Se agregó soporte para los siguientes MongoDB APIs
  - `$literal`
  - `$map`
  - `$$ROOT`
- Soporte para capacidades de GeoSpatial consulta. Consulte esta publicación en el blog para obtener más información
- Compatibilidad para el control de acceso con funciones definidas por el usuario. Consulte esta publicación en el blog para obtener más información
- Controlador JDBC de Amazon DocumentDB para permitir la conectividad desde herramientas de BI como Tableau y herramientas de consulta como SQL Workbench

Correcciones de errores y otros cambios

Amazon DocumentDB 3.6 (versión de parche del motor 1.0.207780) y 4.0 (versión de parche del motor 2.0.5704)

- Se corrigió un error `$natural` para ordenar correctamente cuando había un `.sort()` explícito junto con `$natural`
- Se corrigió un error para que el flujo de cambios funcionara con `$redact`
- Se corrigió un error para que `$ifNull` funcionara con una matriz vacía
- Se ha corregido un error que provocaba una consumption/server caída excesiva de recursos cuando se eliminaba a un usuario que había iniciado sesión en ese momento o se revocaba el privilegio de ese usuario para realizar una actividad en curso
- Se corrigió un error en `listDatabase` y comprobación de privilegios `listCollection`
- Se corrigió un error: lógica de deduplicación para elementos de varias claves

24 de junio de 2021

Nuevas características

Amazon DocumentDB 3.6 (versión de parche del motor 1.0.207117) y 4.0 (versión de parche del motor 2.0.3371)

- Ahora se admiten las instancias r5.8xlarge y r5.16xlarge. Obtenga más información en la publicación en el blog Amazon DocumentDB ahora es compatible con instancias r5.8xlarge y r5.16xlarge.
- Ahora se admiten los clústeres globales para proporcionar recuperación ante desastres tras interrupciones en toda la región y permitir lecturas globales de baja latencia al permitir las lecturas desde el clúster de Amazon DocumentDB más cercano. Tenga en cuenta que los clústeres globales no se admiten en las siguientes regiones: América del Sur (São Paulo), Europa (Milán), China (Pekín) y China (Ningxia).

4 de mayo de 2021

Nuevas características

Consulte todas las nuevas características en esta publicación en el blog.

Amazon DocumentDB 3.6 (versión de parche del motor 1.0.207117) y 4.0 (versión de parche del motor 2.0.3371)

- `renameCollection`
- `$zip`
- `$indexOfArray`
- `$reverseArray`
- `$natural`
- Compatibilidad `$hint` para actualizaciones
- Escaneo de índice para `distinct`

Correcciones de errores y otros cambios

Amazon DocumentDB 3.6 (versión de parche del motor 1.0.207117) y 4.0 (versión de parche del motor 2.0.3371)

- Uso de memoria reducido para consultas `$in`
- Se corrigió una pérdida de memoria en los índices de varias claves
- Se corrigió el plan de explicación y el resultado del generador de perfiles para `$out`
- Se agregó un tiempo de espera para las operaciones del sistema de monitoreo interno para mejorar la fiabilidad
- Se corrigió un defecto que afectaba a los predicados de consulta pasados a índices de varias claves

15 de enero de 2021

Nuevas características

Amazon DocumentDB 4.0 (versión de parche del motor 2.0.722)

- Ninguno

Amazon DocumentDB 3.6 (versión de parche del motor 1.0.206295)

- Posibilidad de utilizar un índice con la etapa de agregación `$lookup`
- Las consultas `find()` con proyecciones se pueden atender directamente desde un índice (consulta cubierta)
- Posibilidad de usar `hint()` con `findAndModify`
- Optimizaciones de rendimiento para el operador `$addToSet`
- Mejoras para reducir el tamaño general de los índices
- Nuevos operadores de agregación: `$ifNull`, `$replaceRoot`, `$setIsSubset`, `$setInstersection`, `$setUnion`, y `$setEquals`
- Los usuarios también pueden finalizar sus propios cursores sin necesidad del rol `KillCursor`

9 de noviembre de 2020

Nuevas características

Consulte todas las nuevas características en esta publicación en el blog.

Amazon DocumentDB 4.0 (versión de parche del motor 2.0.722)

- Compatibilidad con MongoDB 4.0
- Transacciones ACID
- Compatibilidad para `cluster(client.watch()` o `mongo.watch())` y flujos de cambios `(db.watch())` a nivel de la base de datos
- Posibilidad de iniciar o reanudar un flujo de cambios mediante `startAtOperationTime`
- Ampliación del período de retención del flujo de cambios a 7 días (antes era de 24 horas)
- AWS DMS objetivo para Amazon DocumentDB 4.0
- CloudWatch métricas:`TransactionsOpen`,`TransactionsOpenMax`, `TransactionsAbortedTransactionsStarted`, y `TransactionsCommitted`
- Nuevos campos para transacciones en `currentOp`, `ServerStatus`, y `profiler`.
- Posibilidad de utilizar un índice con la etapa de agregación `$lookup`
- Las consultas `find()` con proyecciones se pueden atender directamente desde un índice (consulta cubierta)
- Posibilidad de usar `hint()` con `findAndModify`
- Optimizaciones de rendimiento para el operador `$addToSet`
- Mejoras para reducir los tamaños de los índices generales.
- Nuevos operadores de agregación: `$ifNull`, `$replaceRoot`, `$setIsSubset`, `$setInstersection`, `$setUnion`, y `$setEquals`
- Con los comandos `ListCollection` y `ListDatabase`, ahora puede usar opcionalmente los parámetros `authorizedCollections` y `authorizedDatabases` para permitir a los usuarios enumerar las colecciones y bases de datos a las que tienen permiso de acceso sin necesitar las funciones `listCollections` y `listDatabase`, respectivamente.
- Los usuarios también pueden finalizar sus propios cursores sin necesidad del rol `KillCursor`
- La comparación de tipos numéricos de subdocumentos ya es coherente con la comparación de tipos numéricos de documentos de primer nivel. Amazon DocumentDB ya es compatible con la versión 4.0 de MongoDB.

Amazon DocumentDB 3.6 (versión de parche del motor 1.0.206295)

- Ninguno

Correcciones de errores y otros cambios

Amazon DocumentDB 4.0 (versión de parche del motor 2.0.722)

- `$setOnInsert` ya no permite actualizaciones cuando se utiliza el operador posicional $. Amazon DocumentDB ya es compatible con la versión 4.0 de MongoDB.
- Se solucionó el problema con `$createCollection` y conjunto `autoIndexId`
- Proyección para documentos anidados
- Se modificó la configuración predeterminada de la memoria de trabajo para que se escale con el tamaño de la memoria de la instancia
- Mejoras en la recopilación de elementos no utilizados
- Búsqueda con una clave vacía en la ruta, diferencia de comportamiento con mongo
- Se corrigió un error `dateToString` en el comportamiento de la zona horaria
- Se corrigió `$push` (agregación) para respetar el orden de clasificación
- Se corrigió un error en `$currentOp` con agregado
- Se solucionó un problema de `readPreference` en secundario
- Se solucionó el problema al validar `$createIndex` en la misma base de datos en la que se ejecutó el comando
- Se corrigió un comportamiento incoherente para `minKey`, la búsqueda `maxKey` falla
- Se corrigió el problema por el que el operador `$size` no funcionaba con una matriz compuesta
- Se solucionó el problema de la negación de `$in` con regex
- Se corrigió un error que provocaba que el comando `$distinct` se ejecutara contra una vista
- Se corrigió un problema que provocaba que los comandos de agregación y búsqueda clasificaran los campos que faltan de forma diferente
- Se corrigió el `$eq` en la expresión regular que no verificaba el tipo
- Se corrigió un error `$currentDate` en el comportamiento de la posición ordinal de la marca temporal
- Se fijó la granularidad de milisegundos para `$currentDate`

Amazon DocumentDB 3.6 (versión de parche del motor 1.0.206295)

- Ninguno

30 de octubre de 2020

Nuevas características

Consulte todas las nuevas características en esta publicación en el blog.

Amazon DocumentDB 3.6 (versión de parche del motor 1.0.206295)

- Se agregó la posibilidad de abrir un cursor de flujo de cambios en el nivel del clúster (`client.watch()` o `mongo.watch()`) y la base de datos (`db.watch()`)
- Capacidad de ampliar el período de retención del flujo de cambios a 7 días (antes era de 24 horas)

Correcciones de errores y otros cambios

Amazon DocumentDB 3.6 (versión de parche del motor 1.0.206295)

- Varias mejoras generales en el rendimiento de los casos
- Una mejora de seguridad específica
- Se ha corregido un problema por el que se podía omitir la clasificación en el segundo campo de un índice compuesto
- Habilite el índice normal para garantizar la igualdad en un solo campo de un índice de varias claves (no compuesto)
- Condición de carrera de autenticación fija
- Se ha corregido un problema que provocaba un bloqueo poco frecuente en la recopilación de elementos no utilizados
- Mejoras en la seguridad RBAC
- Añadida la métrica `databaseConnectionsMax`
- Mejoras en el rendimiento de determinadas cargas de trabajo en las instancias `r5.24xlarge`

22 de septiembre de 2020

Nuevas características

Consulte todas las nuevas características en esta publicación en el blog.

Amazon DocumentDB 3.6 (versión de parche del motor 1.0.206295)

- Etapa de agregación `$out`
- Aumentó hasta 10 veces el número máximo de conexiones y de cursores por instancia

Correcciones de errores y otros cambios

Amazon DocumentDB 3.6 (versión de parche del motor 1.0.206295)

- Ninguno

10 de julio de 2020

Nuevas características

Consulte todas las nuevas características en esta publicación en el blog.

Amazon DocumentDB 3.6 (versión de parche del motor 1.0.206295)

- Copia de instantáneas entre regiones

Correcciones de errores y otros cambios

Amazon DocumentDB 3.6 (versión de parche del motor 1.0.206295)

- Ninguno

30 de junio de 2020

Nuevas características

Consulte todas las nuevas características en esta publicación en el blog.

Amazon DocumentDB 3.6 (versión de parche del motor 1.0.206295)

- Instancias medianas T3

Correcciones de errores y otros cambios

Amazon DocumentDB 3.6 (versión de parche del motor 1.0.206295)

- Recuperación de memoria inactiva para instancias t3
- Mejoras en la autenticación
- Rendimiento de autenticación de SASL mejorado
- Se solucionó el problema `currentOp` que se producía al superar el máximo de operaciones
- Se solucionó el problema `killOps` de actualización y eliminación masivas
- Mejoras de rendimiento de `$sample` con `$match`
- Se ha corregido la compatibilidad para `$$` en el segundo caso en la fase de redacción
- Se corrigieron varias causas subyacentes de los bloqueos recurrentes
- Mejoras en el barrido de TTL para reducir IOs la latencia
- Utilización optimizada de la memoria para `$unwind`
- Se corrigió la condición de carrera de estadísticas de colección fija
- Se corrigió la condición de carrera durante la compilación simultánea del índice
- Se corrigió un bloqueo infrecuente en `hash_search` en índice

Historial de documentos de la Guía para desarrolladores de Amazon DocumentDB

- Versión de la API: 2014-10-31
- Última actualización de la documentación: 23 de julio de 2024

En la siguiente tabla se describe la documentación de esta versión de la Guía para desarrolladores de Amazon DocumentDB.

Cambio	Descripción	Fecha
Actualización de políticas administradas de AWS: cambio de política	Amazon DocumentDB actualiza las políticas de acceso completo para los clústeres elásticos.	11 de febrero de 2025
AWS Actualización de políticas administradas de : cambio de política	Amazon DocumentDB actualiza las políticas de acceso completo para los clústeres elásticos.	21 de febrero de 2024
AWS Actualización de políticas administradas de : cambio de política	Amazon DocumentDB actualiza las políticas de solo lectura y acceso completo para los clústeres elásticos.	21 de junio de 2023
AWS Actualización de políticas administradas de : nueva política	Amazon DocumentDB presenta una nueva política de solo lectura para clústeres elásticos.	8 de junio de 2023
AWS Actualización de políticas administradas de : nueva política	Amazon DocumentDB presenta una nueva política de acceso completo para clústeres elásticos.	5 de junio de 2023

Compatibilidad con MongoDB	Amazon DocumentDB ahora es compatible con la versión 5.0 de MongoDB.	1 de marzo de 2023
Actualización de políticas	Para admitir la función de clúster elástico de Amazon DocumentDB, se actualiza la política AmazonDocDBConsoleFullAccess y se introduce la Política de AmazonDocDB-ElasticServiceRolePolicy.	30 de noviembre de 2022
Clústeres elásticos	Se ha añadido una nueva característica de los clústeres elásticos que admite la partición basada en hash (sharding) de datos del sistema de almacenamiento distribuido de Amazon DocumentDB.	30 de noviembre de 2022
Clústeres globales	Se agregó documentación sobre cómo usar los clústeres globales.	2 de junio de 2021
Suscripciones de eventos	Se agregó la documentación de suscripción a eventos.	26 de marzo de 2021
Actualizaciones a la versión	Mejoras documentadas de la versión 3.6 en los controles de acceso basados en roles, los operadores de agregación y el rendimiento.	15 de enero de 2021
Compatibilidad con MongoDB	Amazon DocumentDB ahora es compatible con la versión 4.0 de MongoDB.	9 de noviembre de 2020

Guías de introducción	Nuevas guías de introducción para empezar a utilizar Amazon DocumentDB mediante AWS Cloud9, Amazon EC2, Robo3T o Studio3T.	15 de agosto de 2020
Zonas de disponibilidad adicionales admitidas	Amazon DocumentDB agregó compatibilidad con una zona de disponibilidad adicional en Asia-Pacífico (Seúl) (ap-northeast-2).	14 de julio de 2020
Se ha agregado compatibilidad para la copia de instantáneas entre regiones.	Amazon DocumentDB ha añadido soporte para copiar instantáneas de clústeres entre Regiones de AWS. Para obtener más información, consulte Copiar instantáneas en las regiones.	10 de julio de 2020
Se ha añadido soporte para la clase de instancia T.	Se agregó compatibilidad con los tipos de instancias T3 en todas las regiones que admiten Amazon DocumentDB. Para obtener más información, consulte Clases de instancias admitidas por región y Especificaciones de clases de instancias.	30 de junio de 2020
Se agregó compatibilidad con AWS GovCloud (US).	Amazon DocumentDB ya está disponible en la región AWS GovCloud (US) (EEUU-gob-oeste-1).	29 de junio de 2020

Se agregaron 16 nuevas métricas de CloudWatch.	Amazon DocumentDB agregó soporte para 16 métricas nuevas de Amazon CloudWatch. Para obtener más información, consulte Monitorización del Amazon DocumentDB con CloudWatch.	23 de junio de 2020
Se ha añadido compatibilidad para caracteres nulos y operador $regex.	Amazon DocumentDB ha añadido compatibilidad para caracteres nulos en cadenas y la capacidad de usar un índice para $regex. Para ver las API de MongoDB compatibles y las capacidades de canalización de agregación de Amazon DocumentDB, consulte Diferencias funcionales con MongoDB.	22 de junio de 2020
Se ha agregado compatibilidad para las capacidades mejoradas de indexación con varias claves.	Amazon DocumentDB ha agregado compatibilidad para las capacidades mejoradas de indexación con varias claves, incluidas la indexación de matrices superiores a 2048 bytes y la capacidad de crear un índice compuesto de varias claves con varias claves en la misma matriz. Para obtener más información, consulte Diferencias funcionales con MongoDB.	23 de abril de 2020

Se ha agregado compatibilidad para la protección de eliminación de una pila de CloudFormation de Amazon DocumentDB.	Amazon DocumentDB ha agregado compatibilidad para habilitar la protección de eliminación cuando se crea una pila de Amazon DocumentDB CloudFormation.	20 de abril de 2020
Se ha añadido compatibilidad con control de acceso basado en roles.	Amazon DocumentDB ha añadido compatibilidad con control de acceso basado en roles mediante roles integrados.	26 de marzo de 2020
Se ha añadido compatibilidad para una zona de disponibilidad adicional en Canadá (centro) (ca-centro-1).	Amazon DocumentDB ya está disponible en la región Canadá (centro) (ca-centro-1) con instancias de clase R5 y tres zonas de disponibilidad.	26 de marzo de 2020
Se ha añadido compatibilidad para dos API de MongoDB adicionales.	Amazon DocumentDB añadió compatibilidad con las API de `$dateFromString` y MongoDB `executionStats`.	23 de marzo de 2020
Se ha agregado compatibilidad con cinco API de MongoDB adicionales.	Amazon DocumentDB añadió compatibilidad con las API de `$objectToArray`, `$arrayToObject`, `$slice`, `$mod` y MongoDB `$range`.	6 de febrero de 2020
Se ha añadido compatibilidad con Canadá (centro).	Amazon DocumentDB ya está disponible en la región Canadá (centro) (ca-centro-1) con instancias de clase R5.	11 de diciembre de 2019

Se ha añadido compatibilidad con ChangeStreamLogSize.	Amazon DocumentDB ha añadido soporte para `ChangeStreamLogSize` para las métricas de Cloudwatch.	22 de noviembre de 2019
Compatibilidad añadida con la región Europa (París	Amazon DocumentDB ya está disponible en la región Europa (París) (eu-oeste-3) con instancias de clase R5.	30 de octubre de 2019
Compatibilidad añadida con la región de Asia-Pacífico (Bombay	Amazon DocumentDB ahora está disponible en la región Asia-Pacífico (Bombay) (ap-sur-1) con instancias de clase R5.	17 de octubre de 2019
Compatibilidad añadida con tres API de MongoDB adicionales	Amazon DocumentDB agregó compatibilidad con las API de `$addFields` , `$concatArrays` , de `$lookup` MongoDB.	16 de octubre de 2019
Compatibilidad añadida con la región de Asia-Pacífico (Singapur	Amazon DocumentDB ahora está disponible en la región Asia-Pacífico (Singapur) (ap-sur-1) con instancias de clase R5.	14 de octubre de 2019
Se añadió un nuevo documento para actualizar certificados TLS	Se añadieron instrucciones para actualizar los certificados de CA de tal forma que se utilice el nuevo para crear las conexiones TLS.	2 de octubre de 2019

Se añadió soporte de API para los certificados	Amazon DocumentDB incorpora un nuevo tipo de certificado de datos para las instancias. Para obtener más información, consulte DBInstance.	1 de octubre de 2019
Compatibilidad con la creación de perfiles de consultas	Amazon DocumentDB ha añadido la posibilidad de crear un perfil de las operaciones admitidas en las instancias y bases de datos del clúster.	19 de agosto de 2019
Se agregó una tercera zona de disponibilidad en Asia-Pacífico (Tokio)	Amazon DocumentDB agregó una tercera zona de disponibilidad (AZ) para sus instancias informáticas en Asia Pacífico (Tokio).	9 de agosto de 2019
Compatibilidad con API de Mongo adicionales	Se agregó soporte para capacidades de canalización de agregación adicionales que incluyen los operadores `$in`, `$isoWeek`, `$isoWeekYear` , `$isoDayOfWeek` , así como operadores de agregación `$dateToString` y la etapa de agregación `$addToSet` . Amazon DocumentDB también agregó compatibilidad con el comando `top()` para el diagnóstico a nivel de colección y la posibilidad de modificar el parámetro `expireAfterSeconds` de los índices TTL mediante el comando `collMod()` .	31 de julio de 2019

Compatibilidad añadida para la región Europa (Londres)	Amazon DocumentDB ya está disponible en Europa (Londres) (eu-oeste-2) con instancias de clase R5.	18 de julio de 2019
Se han añadido muestras de código	Se han añadido ejemplos de código en R y Ruby para la conexión mediante programación a Amazon DocumentDB.	17 de julio de 2019
Se ha añadido una práctica recomendada	Se ha añadido una práctica recomendada para ayudarle a administrar sus costos de Amazon DocumentDB.	17 de julio de 2019
Compatibilidad con la detención e inicio de un clúster	Amazon DocumentDB ha incluido compatibilidad con la detección e inicio de clústeres para administrar los costos de entornos de desarrollo y pruebas.	1 de julio de 2019
Compatibilidad con la protección contra eliminación del clúster	Amazon DocumentDB ha incluido la protección contra eliminación para proteger sus clústeres contra la eliminación accidental. Para obtener más información, consulte los siguientes temas: Creación de un clúster de Amazon DocumentDB, Modificación de un clúster de Amazon DocumentDB, Eliminación de un clúster de Amazon DocumentDB, y `DeletionProtection` en el tema de la API DBCluster.	1 de julio de 2019

Actualización de diferencias funcionales	Se han añadido transacciones implícitas a las diferencias funcionales.	26 de junio de 2019
Adición de diferencias funcionales	Se ha añadido una nota en relación con el almacenamiento y la compresión del índice en Amazon DocumentDB.	13 de junio de 2019
Se ha añadido compatibilidad con más regiones	Amazon DocumentDB ya está disponible en la Asia-Pacífico (Sídney) (ap-sureste-2) con instancias de clase R5.	5 de junio de 2019
La clase de instancia R5 se admite en regiones adicionales	Se ha añadido compatibilidad con la clase de instancia R5 en otras 4 regiones: Este de EE. UU. (Ohio), Este de EE. UU. (Norte de Virginia), Oeste de EE. UU. (Oregón) y UE (Irlanda). Con este cambio, las instancias R5 se admiten en todas las regiones que admiten Amazon DocumentDB.	17 de mayo de 2019

Regiones adicionales compatibles	Se ha añadido compatibilidad con 2 regiones adicionales, Asia-Pacífico (Tokio) (ap-noreste-1) y Asia-Pacífico (Seúl) (ap-noreste-2), con clases de instancias R5. Para obtener más información, consulte Clases de instancias admitidas por región y Especificaciones de clases de instancias.	8 de mayo de 2019
Se han añadido más ejemplos del código de conexión	Se han añadido ejemplos de código en Java y C# para conectarse a Amazon DocumentDB.	24 de abril de 2019
Soporte adicional para la API de Mongo	Se ha añadido compatibilidad adicional con siete operadores de cadenas de agregación (`$indexOfBytes`, `$indexOfCP`, `$strLenBytes`, `$strLenCP`, `$toLower`, `$toUpper`, y `$split`), nueve operadores de fecha y hora (`$dayOfYear`, `$dayOfMonth`, `$dayOfWeek`, `$year`, `$month`, `$hour`, `$minute`, `$second`, y `$millisecond`) y la etapa de canalización de agregación `$sample`.	4 de abril de 2019
Se han añadido ejemplos del código de conexión	Se han añadido ejemplos de código en Python, Node.js, PHP y Go para conectarse a Amazon DocumentDB.	21 de marzo de 2019

Compatibilidad con la región de Fráncfort e instancias R	Se ha añadido compatibilidad con la región Europa (Fráncfort) (eu-centro-1) con clases de instancias R5. Para obtener más información, consulte Clases de instancias admitidas por región y Especificaciones de clases de instancias.	13 de marzo de 2019
Compatibilidad con operadores de canalización de agregación	Se ha añadido compatibilidad con nuevos operadores de cadenas de agregación (`$concat`, `$substr`, `$substrBytes` , `$substrCP` , `$strcasecmp`), un operador de agregación de matriz (`$size`), un operador de acumulador de grupo de agregación (`$push`) y etapas de agregación (`$redact` y `$indexStats`). También se ha añadido compatibilidad con operadores de matriz posicional (`$[]` y `$[<identifier>]`) y `hint()`.	28 de febrero de 2019
Actualizaciones del motor	Se ha añadido documentación para determinar las modificaciones del clúster pendientes y para actualizar la versión del motor del clúster.	15 de febrero de 2019
Auditoría de eventos	Se ha añadido compatibilidad para auditar eventos de bases de datos con Registros de Amazon CloudWatch.	12 de febrero de 2019

Quick Start (Inicio rápido	Se ha añadido un tema de inicio rápido para ayudarle a comenzar a utilizar fácilment e Amazon DocumentDB con CloudFormation.	11 de enero de 2019
Versión pública	Esta es la versión pública inicial de Amazon DocumentD B (con compatibilidad con MongoDB). Esta versión incluye la Guía para desarroll adores y la Referencia de la API para administración de recursos.	9 de enero de 2019

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.